National Aeronautics and Space Administration
Ames Research Center
Moffett Field, California 94035

NASA Certification Authority
Certification Practice Statement

April 2, 2002
Revision 1.3.1.1

National Aeronautics and Space Administration
Ames Research Center
Applied Information Technology Division
Moffett Field, CA. 94035-1000

NASA Certification Authority Certification Practice Statement

Signature:

___________________________ _______________

NASA Chief Information Officer Date

Table of Contents

1. Introduction

The National Aeronautics and Space Administration (NASA) operates a Public Key Infrastructure (PKI) to provide security for its electronic information. Programs that carry out or support NASA's missions may require the type of security services provided by a PKI. A PKI is a complex system that provides secure electronic data storage and exchange. Security is achieved by using public key cryptography. The types of security services provided by a PKI are:

- Confidentiality: The transformation of data into a form unreadable by anyone without the proper key
- Data Integrity: A service that addresses the unauthorized alteration of data by either confirming its integrity or warning about changes
- Authentication: The process whereby users or information sources prove that they are who they claim to be
- Non-repudiation: A service that limits denial of previous commitments or actions

These services are provided through public key cryptography's use of certificates and the public and private cryptographic keys associated with the certificates.

The primary function of a PKI is to manage these certificates and keys. A PKI manages the certificates through the following components:

- Certification Authority (CA): A trusted party that creates, renews, and revokes certificates.
- Registration Authority (RA): A trusted agent of the CA that verifies user identity.
- Certificate Repository*:* The public area in which users' public keys are stored. This is usually a directory such as X.500.
- Policy*.* The set of rules that guide the operation of the PKI.

The NASA PKI consists of a central NASA CA, RAs at each of the eleven NASA centers, and an X.500 directory for each NASA center. The documents that define the policy are the X.509 Certificate Policy (CP) for the NASA PKI and the NASA Certification Authority Certification Practice Statement (CPS).

This document describes the certification practices that have been implemented by the NASA Certificate Authority (CA). This CPS includes:

- Subscriber identification and authorization verification
- Control of PKI computer and cryptographic systems
- Operation of PKI computer and cryptographic systems, facilities and personnel
- Usage of keys and public-key certificates by Subscribers and Relying Parties
- Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this CPS are being met

This CPS has been drafted to comply with the requirements of the X.509 Certificate Policy (CP) for NASA Public Key Infrastructure (PKI). The relationship between the X.509 Certificate Policy for NASA PKI and this CPS is the CP states the policies of a NASA CA and this CPS provides the implementation details of the CP. Please note, definitions of terms used in this CPS are provided in Appendix B. Terms defined in Appendix B are underlined the first time they appear in this CPS.

To obtain information concerning the underlying policies for this CPS, please consult the X.509 Certificate Policy for NASA Public Key Infrastructure (PKI).

1.1 OVERVIEW

This CPS follows and complies with the Internet Engineering Task Force (IETF) Request for Comment (RFC) 2527, X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

This CPS is intended for use by the National Aeronautics and Space Administration (NASA) and others who need to assess the trustworthiness of the NASA CA and determine the suitability of its certificates in meeting their requirements for electronic information security.

This CPS describes the primary obligations and operational responsibilities of all NASA PKI program participants, and defines the creation, management and use of Version 3 X.509 public key certificates. Public key certificates are appropriate for use in applications requiring communication between networked computer-based systems and applications requiring electronic information integrity and confidentiality. Such applications include, but are not limited to, electronic mail; transmission of unclassified but sensitive information; digital signing of electronic forms; contract submission digital signatures; and authentication of infrastructure components such as web servers. Please note, the term, “X.509 certificates”, as used within this CPS implies X.509 version 3 certificates. Also note, the term, “PKI client software” refers to the software that provides PKI functionality within the NASA CA domain. While this CPS does not require the use of public key certificates in any particular NASA application or program, if public key certificates are used they must be used in accordance with this CPS and the X.509 Certificate Policy for NASA PKI.

This CPS supports medium level assurance, unless specified otherwise. As NASA adds other assurance levels, this CPS will be modified to describe the policies for these levels. Please note that the term, “assurance”, refers to the level of trust associated with a certificate.

Issuance of a public key certificate under any of this CPS

- is not to be used for protection of classified information;
- does not imply that the Subscriber has any authority to conduct business transactions on behalf of the organization operating the NASA CA.

The terms and provisions of this CPS shall be interpreted under and governed by United States Federal law. The United States Government disclaims any liability that may arise from the use of this CPS.

1.1.1 NASA PKI Organization

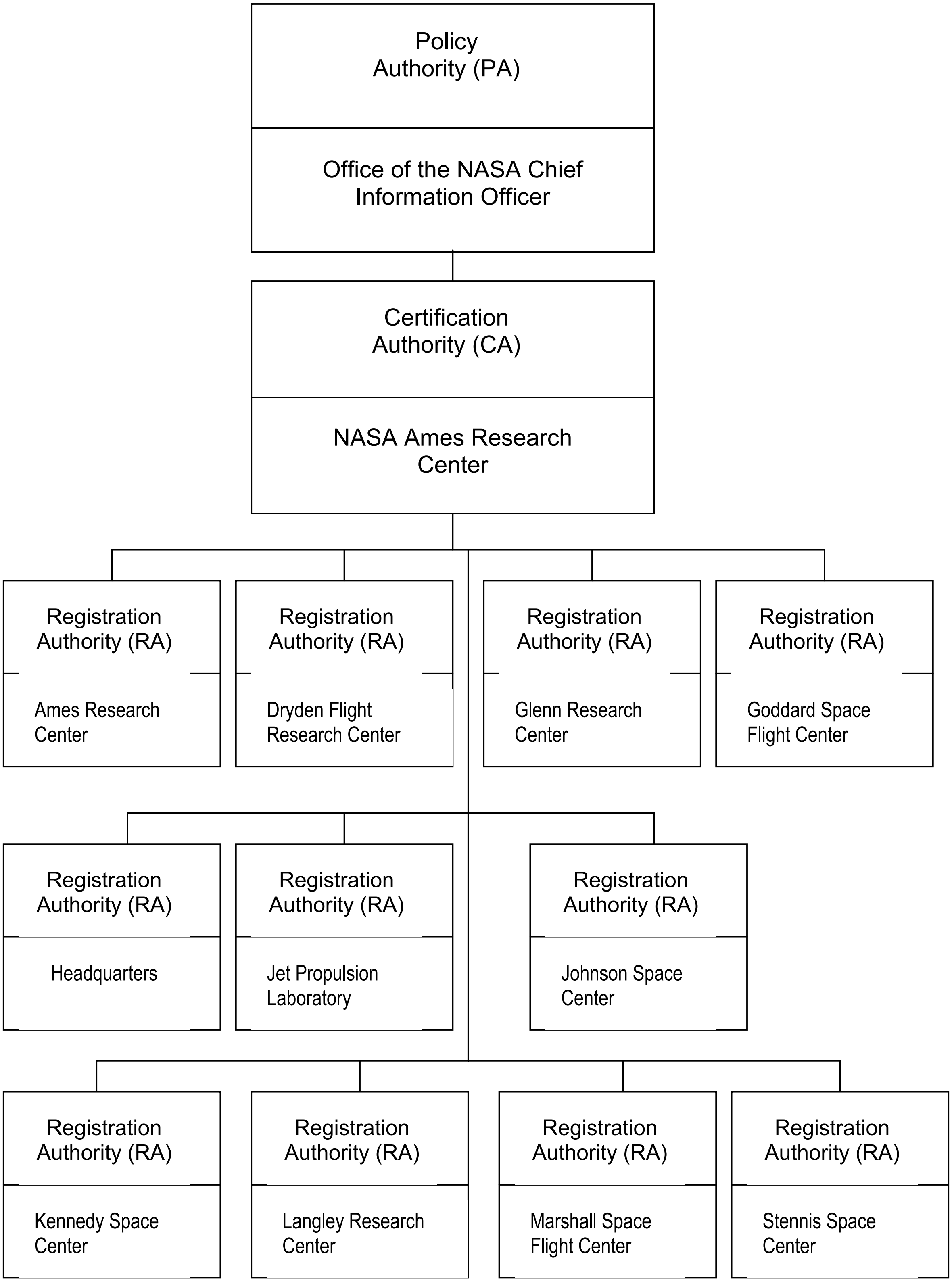
The NASA Policy Authority (PA) is responsible for the overall management of the NASA PKI. The NASA PA is responsible for defining the policies under which the NASA PKI operates. The NASA PA duties include ensuring that NASA CA's operate in accordance with policies and practices defined in relevant Certification and Certificate documents, and approving and administering cross-certifications. The NASA PA is vested in the Office of the NASA Chief Information Officer.

The NASA Certificate Authority (CA) is responsible for the creation and management of Version 3 X.509 public-key certificates for use by NASA and in accordance with the NASA CP and this CPS. Ames Research Center (ARC) is appointed by the NASA CIO, as the NASA CA in virtue of ARC's role as the Principal Center for Information Technology (IT) security.

NASA uses local Registration Authorities (RAs) to collect information, verify identity and authorize, and request certificate management actions on behalf of their Subscriber population. Each of the eleven NASA Centers is responsible for operating a RA.

The diagram on the following page depicts the general concept of the NASA PKI.

NASA PKI ORGANIZATION


Policy Authority (PA)
Office of the NASA Chief Information Officer
Certification Authority (CA)
NASA Ames Research Center
Registration Authority (RA)
Ames Research Center
Registration Authority (RA)
Dryden Flight Research Center
Registration Authority (RA)
Glenn Research Center
Registration Authority (RA)
Goddard Space Flight Center
Registration Authority (RA)
Headquarters
Registration Authority (RA)
Jet Propulsion Laboratory
Registration Authority (RA)
Johnson Space Center
Registration Authority (RA)
Kennedy Space Center
Registration Authority (RA)
Langley Research Center
Registration Authority (RA)
Marshall Space Flight Center
Registration Authority (RA)
Stennis Space Center

1.2 IDENTIFICATION

Upon identification by the NASA PA, the applicable object identifiers (OIDs) will be included in NASA certificates. In the area of level of assurance, OIDs will be used to indicate the level of assurance associated with a certificate. The NASA CA will use the Federal Public Key Infrastructure four levels of assurance, rudimentary, basic, medium and high.

1.3 COMMUNITY & APPLICABILITY

This CPS defines the practices under which the NASA CA is administered and operated.
The NASA CA is a Certification Authority within the NASA PKI, as directed by the NASA PA.

1.3.1 Certification Authority (CA)

The NASA CA is operated by Ames Research Center (ARC) as appointed by the NASA Chief Information Officer and in collaboration with the Enterprise Associate Administrators and the Institutional Program Offices.

NASA PKI Operations within the Applied Information Technology Division at Ames Research Center is responsible for the overall operation of the NASA CA. NASA PKI Operations is also responsible for the maintenance and administration of this CPS, and review of the operations of the RAs within the NASA CA domain. NASA PKI Operations reports to the NASA PA regarding issues of CA operation.

The NASA CA is intended for use within NASA and potentially with organizations or individuals that are outside of NASA but have business or research relationships with NASA.

The NASA CA issues, signs and manages public key certificates. The CA issues certificates to all NASA employees and contractors on an as-needed basis. The NASA CA issues cross-certificates to CAs operated by other federal or state facilities, contractors, suppliers, and customer organizations as needed to support NASA business processes. Approval for the issuance of cross-certificates is obtained from the NASA PA.

The NASA CA is responsible for:

- creating End Entity Confidentiality (encryption) key pairs;
- creating and signing of X.509 certificates binding Subscribers with their public keys;
- creating and signing certificates with other Certification Authorities (with approval from the NASA PA);
- promulgating certificate status through CRLs;
- operating the CA in accordance with this CPS;
- approving and assigning individuals to fulfill the CA Master User and CA Officer positions;
- reviewing and auditing RA operations within its domain;
- resolving disputes between Subscribers and the CA or RA;
- requesting revocation of PKI Officer's or RAs' certificate;

The NASA CA includes people who are responsible for the overall operation of the CA and people who operate and maintain the CA server and the CA software.
The CA Master Users and the CA Officers are responsible for the operation and administration of the CA server and CA software, respectively.

When necessary, this CPS distinguishes the roles accessing the CA functions. When this distinction is not required, the term CA is used to refer to the total CA entity, including the software and its operations.

Across certification between the NASA CA and another CA shall be in accordance with the X.509 Certificate Policy for NASA PKI and this CPS and any additional requirements determined by the NASA PA. All cross certification will be done pursuant to instructions from the NASA PA. Any agreements made with other CAs shall be documented and applicable disclaimers made available to Subscribers.

1.3.2 Registration Authorities (RAs)

A Registration Authority (RA) is responsible for End Entity administration on behalf of the NASA CA. Each NASA Center is responsible for establishing and operating a center-wide RA. At each NASA Center under the NASA CA domain, the Center Director appoints, in writing, the Registration Authority personnel.

The RA is responsible for:

- identifying and authenticating the identity of certificate applicants;
- receiving and distributing Subscriber authorization information;
- performing certificate and key management functions for their Subscriber population (i.e. enabling and disabling/suspending certificates, updating certificates/keys, revoking certificates and managing key recovery for Subscribers;
- changing Subscriber's Distinguished Name (DN) on the certificate. Changing Subscriber's DN is done with the cooperation and assistance of the Center's X.500 Directory Administrator;
- viewing audit logs and reporting suspicious events to the CA Officers; and
- creating various reports of Subscriber status.

The term RA is used to refer to an individual within each NASA Center with RA privileges who performs the RA functions.

1.3.3 End Entities

1.3.3.1 SUBSCRIBERS

A Subscriber is the entity whose name appears as the subject in a certificate. Subscribers use private keys issued and/or certified by the NASA CA for approved applications. Subscribers include NASA employees and contractors. Special considerations for non-NASA employees or contractors, including foreign nationals, must comply with NASA Procedures and Guidelines (NPG) number 2810.1 titled "Security of Information Technology".

A certificate may be issued to a non-human End Entity, e.g. a process or a server. In this case, the person who is responsible for this non-human End Entity needs to apply and maintain a certificate for this entity.

In addition, Subscribers may use certificates issued by the NASA CA to encrypt information for, and verify the digital signatures of, other Subscribers (within the NASA CA domain as well as cross-certified domains). As such, Subscribers are also Relying Parties.

In this CPS, the term End Entity is used to represent users in general including their roles as Subscribers and Relying Parties. No End Entities are only Subscribers and no End Entities are only Relying Parties in the NASA PKI. Where separation of these roles is required in this CPS, the term Subscriber is used to refer to an End Entity as a certificate subject, while Relying Party is used to refer to an End Entity verifying certificates issued by the NASA CA.

1.3.3.2 RELYING PARTIES

A Relying Party is an entity that relies on the validity of the binding of the Subscriber’s name to a public key. A Relying Party may be either a certificate subject of the NASA CA or a Subscriber of an external CA that has signed a cross certification agreement with the NASA CA. The rights and obligations of a Relying Party who is a certificate subject of the NASA CA are covered in this CPS. The rights and obligations of a Relying Party belonging to an external CA are covered by the cross certification agreement between the two CAs.

1.3.4 Applicability

The practices described in this CPS apply to the NASA CA and its administrators, the NASA RAs and their administrators, the repository used by the NASA CA, to End Entities certified by the NASA CA, and to Relying Parties.

Certificates issued under this CPS shall only be used for transactions relating to NASA business. Certificates issued under this CPS are suitable for providing confidentiality, electronic authentication, authorization and data integrity for NASA information up to and including Sensitive Unclassified

The combination of this CPS and associated certificates, can be used to protect NASA sensitive unclassified data including:

- mission information
- information that NASA is required by law or agreement to protect such as Privacy Act
- information and information provided to NASA by its contractors and subject to non-disclosure agreement
- proprietary business and technology information such as legal, payroll, personnel and contract proposal and source selection information
- electronic commerce transactions including EDI, e-mail, Web servers, SSL, etc.
- personnel information, including position, salary, benefits, health

1.3.5 Approved And Prohibited Applications

Applications for which issued certificates are suitable include the following:

- Applications that use or contain NASA sensitive unclassified information.
- Electronic mail applications that use NASA standard electronic mail packages.
- Web applications that contain NASA sensitive unclassified information.
- Electronic forms used in conducting NASA business.

Applications for which issued certificates are prohibited include the following:

- Applications that use or contain classified information.
- Applications that have no relevance to NASA business.

Approved and prohibited applications are identified by the NASA PA.

1.3.6 Repositories

The NASA CA uses the NASA X.500 Directory to publish and distribute certificates, Certificate Revocation Lists (CRLs) and Authority Revocation Lists (ARLs). Marshall Space Flight Center manages the NASA X.500 directory. The directory is available 24 hours a day with operational support available 12 hours a day, 5 days a week.

The NASA X.500 Directory is composed of a top level Directory Service Agent (DSA) and individual X.500 directories for each NASA Center. The top level or NASA level DSA holds the CRLs and ARLs. The NASA level DSA distributes End Entity certificates to the appropriate NASA Center X.500 directory (for example: an End Entity that is employed by Ames Research Center would have its certificate published in the Ames X.500 Directory). Each NASA Center has its own X.500 directory administrator to support their respective X.500 directories.

The NASA CA maintains a repository for NASA PKI supported certification policies and this CPS (see section 2.6.4).

1.4 CONTACT DETAILS

This CPS is administered by the NASA PKI Operations, Applied Information Technology Division, Ames Research Center.

The contact person is:
Chairman, NASA PKI Operations
Applied Information Technology Division
MS: 233-10
Ames Research Center
Moffett Field, CA 94035-1000

2. General Provisions

2.1 Obligations

2.1.1 CA Obligations

The NASA CA will operate in accordance with this CPS, the X.509 Certificate Policy for NASA PKI, and U.S. Federal law and regulations when issuing and managing the keys provided under this CPS.

The NASA CA is obliged to:

- establish, maintain and publish a Certificate Practice Statement;
- provide CA services in accordance with the practices described in this CPS;
- CA server services are provided 7days a week, 24 hours per day with the stipulation that this is not a warranty of 100% availability. Availability may be affected by system maintenance, system repair, or by factors outside the control of the CA.
- issue certificates to NASA employees, contractors, and to other CAs, in accordance with the practices referenced in this CPS and the X.509 Certificate Policy for NASA PKI;
- revoke certificates upon receipt of a valid request to do so, in accordance with the practices this CPS and the X.509 Certificate Policy for NASA PKI;
- provide encryption key recovery services, in accordance with the practices this CPS and the X.509 Certificate Policy for NASA PKI;
- issue and publish CRLs and ARLs on a regular schedule as per this CPS and the X.509 Certificate Policy for NASA PKI;
- notify others (e.g. Relying Parties) of certificate issuance/revocation by provision of access to certificates, CRLs, and ARLs in the NASA CA repository;
- ensure awareness of and adherence to this CPS within the NASA CA's Subscriber and RA communities through publication of the CPS and X.509 Certificate Policy for NASA PKI and audit of RA's within the NASA CA domain;
- in concert with the NASA PA ensuring corrective actions to CA or RA deficiencies identified by an audit. Reporting status of corrective actions to the NASA PA;
- establish that any CA with whom it cross-certifies complies with all CPs that are mutually recognized; and
- through compliance audit, verify to cross-certifying CAs that it complies with the X.509 Certificate Policy for NASA PKI.

Limitations to the NASA CA obligations are as follows:

The NASA CA is not liable for loss:

- of CA or RA service due to war, natural disasters or other uncontrollable forces.
- incurred between the time a certificate is revoked and the next scheduled issuance of a CRL.

- due to unauthorized use of certificates issued by the NASA CA, and use of certificates beyond the authorized uses defined by the X.509 Certificate Policy for NASA PKI and this CPS.
- caused by fraudulent or negligent use of certificates and/or CRLs and/or ARLs issued by the NASA CA.
- due to disclosure of personal information contained within certificates and/or CRLs and/or ARLs

2.1.1.1 NOTIFICATION OF CERTIFICATE ISSUANCE AND REVOCATION

Upon creation, a Subscriber's certificate is published in the NASA X.500 directory. When a Subscriber's certificate is revoked it is written to the Certificate Revocation List and published in the NASA X.500 directory.

2.1.1.2 ACCURACY OF REPRESENTATIONS

By publishing a certificate in the NASA X.500 directory, the NASA CA certifies it has issued a certificate to the named Subscriber; and that the information stated in the certificate was verified in accordance with this CPS; and the Subscriber has accepted the certificate.

The NASA CA provides notification of a Subscriber's and Relying Party's rights and obligations under this CPS through the publication of this CPS and the X.509 Certificate Policy for NASA PKI. In addition, the NASA PKI Subscriber Agreement describes Subscriber obligations and responsibilities.

2.1.1.3 TIME BETWEEN CERTIFICATE REQUEST AND ISSUANCE

The RA at each NASA Center is responsible for processing certificate requests. The time between the acceptance of the certificate request and issuance will vary depending on the Center's staffing and hours of operation as well as the time required to verify the Subscriber's identity.

When the RA has verified the Subscriber's identity and accepted the certificate request, the RA logons to the CA server to process the certificate request. The NASA CA will immediately return authorization data to the RA. Each Center's RA will notify the requester when the certificate request has been approved and authorization data can be obtained.

2.1.1.4 CERTIFICATE REVOCATION AND RENEWAL

The RA at each NASA Center is responsible for processing certificate revocations and renewals. Certificate revocation must be requested in writing to the local RA. When the RA logons to the CA server to process the revocation, the NASA CA will update the CRL immediately. The local RA will inform the revocation requester as soon as practicable.

Revoked certificates are published in CRLs and posted to the NASA X.500 directory, in accordance with section 4.4.9 of this CPS. RAs can immediately post a CRL if deemed necessary.

Certificate renewals as part of routine re-key are issued automatically by the NASA CA for NASA employees (i.e. civil servants) only.

2.1.1.5 Protection Of Private Keys

The NASA CA protects its private keys and activation data in accordance with the provisions of sections 4 and 6 of this CPS.

The NASA CA protects the private keys it holds or stores and the activation data in accordance with sections 4 and 6 of this CPS.

2.1.1.6 Restrictions On Issuing CA'S Private Key Use

The NASA CA's signing key is used only for CA related activities such as signing certificates, CRLs and ARLs.

The NASA CA may issue and sign cross certificates with other CAs only as expressly authorized by the NASA PA.

2.1.2 RA Obligations

The NASA RAs within the NASA CA domain are obligated to conform to the stipulations of this CPS and the X.509 Certificate Policy for NASA PKI.

The RAs are obliged to:

- verify the accuracy and authenticity of the information provided by requesters for a certificate. The RAs provide this verification on behalf of the NASA CA.
- request revocation of a Subscriber's certificates in accordance with the stipulations in this CPS.
- provide RA services to their respective Center. Hours of operation for the RA will be locally determined by each Center.
- ensure the RA services are in accordance with the stipulation of the relevant practices of this CPS and the X.509 Certificate Policy for NASA PKI.
- be accountable for transactions performed on behalf of the CA.
- bring to the attention of their Subscribers all relevant information pertaining to the rights and obligations of the CA, RA and Subscriber contained in this CPS, the Subscriber Agreement, and any other relevant document outlining the terms and conditions of use.

An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

2.1.2.1 Notification Of Certificate Issuance And Revocation

The RA at each NASA Center is obligated to conform to certificate issuance and revocation stipulations of this CPS and the X.509 Certificate Policy for NASA PKI.

The RA at each NASA Center is responsible for processing requests for certificate issuance and revocation. Each Center's RA will notify the requester when the request has been approved and if any subsequent action is required by the requester.

The RAs do not have to notify a Relying Party of the issuance or revocation of a certificate.

2.1.2.2 ACCURACY OF REPRESENTATIONS

When the RA logons to the CA server to process a certificate request, the RA is certifying that it has authenticated the identity of that Subscriber in accordance with the practices described in sections 3 and 4 of this CPS.

2.1.2.3 PROTECTION OF RA PRIVATE KEY

Each RA must ensure that his or her private keys are protected in accordance with the controls described in section 6 of this CPS.

2.1.2.4 RESTRICTIONS ON RA PRIVATE KEY USE

RAs use of their private keys are restricted to official NASA business and only for purposes authorized by the X.509 Certificate Policy for NASA PKI and in conformance with this CPS.

2.1.3 Subscriber Obligations

In the NASA CA domain, End Entities are both Subscribers and Relying Parties. As Subscribers, they are obliged to:

- make true representation at all times to both the NASA CA and RA regarding information in their certificates and other identification and authentication information;
- use certificates exclusively for legal and authorized NASA business, consistent with the X.509 Certificate Policy for NASA PKI and this CPS;
- take reasonable precautions to protect their private keys and key tokens (if applicable) from loss, disclosure, modification, or unauthorized use;
- protect private decryption keys and private signing keys through cryptographic mechanisms or storing them on a hardware token or a diskette. (Within the NASA PKI, the NASA PKI software protects a subscriber’s private keys through cryptographic mechanisms.) The Subscriber may further protect his/her private keys by storing them on a hardware token or diskette and, when not in use, removing the token or diskette from the computer and keeping the token or diskette on his/her person or stored in a secure, locked container or drawer;
- protect their user password, by not writing it down and not disclosing their password to others. If a Subscriber is concerned about not remembering the password, he/she may store a written copy in a secure, locked container or drawer;.
- inform their local RA within 48 hours of a change to any information included in their certificate or certificate application request;
- inform their local RA within 8 hours of a suspected compromise of one/both of their private keys; and
- inform their local RA when the Subscriber no longer requires the certificate, for reasons including job transfer, extended leave, resignation or termination of employment.

By adhering to the practices described in this CPS and the NASA PKI Subscriber Agreement, Subscribers fulfill the obligations imposed upon them by the policies under which their certificates are issued.

2.1.3.1 ACCURACY OF REPRESENTATIONS

By signing a certificate request (i.e. issuance, revocation, recovery), a Subscriber certifies to the NASA CA and RA that any information submitted to the CA or RA is complete and accurate.

2.1.3.2 PROTECTION OF SUBSCRIBER PRIVATE KEY AND KEY TOKEN

Subscribers are required to protect their private keys and key tokens (if applicable) in accordance with the practices in section 6 of this CPS. Subscribers must take reasonable precautions to prevent loss, disclosure, modification, or unauthorized use of their private keys.

If private keys are stored on a token, Subscribers must remove the token from the computer when not in use, and keep the token on their person or stored in a secure, locked container.

2.1.3.3 RESTRICTIONS ON SUBSCRIBER PRIVATE KEY USE

Subscriber will use the keys and certificates only for purposes related to NASA business and in conformance with the X.509 Certificate Policy for NASA PKI and this CPS.

2.1.3.4 NOTIFICATION UPON PRIVATE KEY COMPROMISE

When a Subscriber suspects private key compromise, he or she must immediately notify his or her local RA within 8 hours and in accordance with the practices described in section 4 of this CPS.

2.1.4 Relying Party Obligations

In the NASA CA domain, End Entities are both Subscribers and Relying Parties. As Relying Parties, they are obliged to:

- restrict use and reliance on certificates issued by the NASA CA to appropriate uses for those certificates, in accordance with the X.509 Certificate Policy for NASA PKI and in accordance with this CPS.
- verify certificates, including checking the CRLs and ARLs, taking into account any critical extensions. (Verification of certificates is in accordance with the certification path validation procedure specified in ITU-T Recommendation X.509 *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework* ISO/IEC 9594-8 (1997)). (Within the NASA PKI, the NASA PKI software checks the CRLs and ARLs to confirm certificate validity.)
- use and rely on certificates only if a valid certificate chain is established between the Relying Party and the certificate subject.

By adhering to the practices described in this CPS, Relying Parties fulfill the obligations imposed upon them by the policies under which their certificates are issued.

2.1.4.1 USE OF CERTIFICATES FOR APPROPRIATE PURPOSE

Relying Parties must use the certificate only for the purposes for which it was issued and in accordance with the X.509 Certificate Policy for NASA PKI and this CPS.

2.1.4.2 VERIFICATION RESPONSIBILITIES

Relying Parties are responsible for validating the NASA CA's signature and the expiration date on a certificate prior to relying on the associated public key. In addition the Relying Party is responsible for verifying the Subscriber's digital signature prior to accepting digitally signed data. Verification should be performed via the PKI software.

Where verification is performed automatically by a cryptographic process and supporting hardware/software installed on the Relying Parties' workstation, Relying Parties should ensure that they are using approved software.

2.1.4.3 REVOCATION CHECK RESPONSIBILITY

Prior to using a certificate, Relying Parties are required to check the certificate status against a current CRL. The relying parting must verify the digital signature of the CRL to ensure it was signed by the NASA CA.

2.1.5 Repository Obligations

CRLs are available to Relying Parties in accordance with practices described in section 4.4.9 of this CPS.

2.2 LIABILITY

NASA disclaims any liability that may arise from use of any certificate issued by or under the authority of NASA, or from the determination to revoke a certificate issued by or under the authority of NASA. In no event will NASA be liable for any damages, including, but not limited to, direct, indirect, special, consequential or punitive damages, arising out of or relating to any certificate issued or revoked by or under the authority of NASA.

2.3 FINANCIAL RESPONSIBILITY

2.3.1 Indemnification By Relying Parties

No stipulation.

2.3.2 Fiduciary Relationships

Issuance of certificates by the NASA CA and assistance in that issuance by NASA RAs does not make NASA or its CA or RAs an agent, fiduciary, trustee, or other representative of requesters or Relying Parties, or others using the NASA PKI.

2.4 Interpretation & Enforcement

2.4.1 Governing Law

United States Federal law shall govern the enforceability, construction, interpretation, and validity of this CPS.

2.4.2 Severability, Survival, Merger, Notice

Severance or merger may result in changes to the scope, management and/or operation of the NASA CA. In such an event, the X.509 Certificate Policy for NASA PKI and this CPS may require modification as well. Should it be determined that one section of this CPS is incorrect or invalid, the other sections of this CPS shall remain in effect until the CPS is updated. Requirements for updating this CPS are described in section 8 of this CPS. Responsibilities, requirements, and privileges of this CPS are merged to the newer CPS upon its release.

2.4.3 Dispute Resolution Procedures

Any dispute related to key and certificate management between NASA and an organization or individual outside of NASA shall be resolved using an appropriate dispute settlement mechanism. The dispute shall be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved through arbitration by the NASA PA.

Within the NASA CA domain, disputes between NASA users, one of which acts in the role of a Subscriber and the other which acts in the role of a Relying Party, or between NASA users and the CA or RA, shall initially be reported to the NASA PKI Operations for resolution.

2.5 Fees

No stipulation.

2.6 Publication & Repository

2.6.1 Publication of CA Information

The NASA CA publishes the following:

- all encryption and signing public key certificates issued by the NASA CA are published in the NASA X.500 Directory
- all cross-certificates issued by the NASA CA to other CAs are published in the NASA X.500 Directory
- the most recent CRL of public key certificates that have been revoked by the NASA CA are published in the NASA X.500 Directory
- the most recent ARL of cross-certificates that have been revoked by the NASA CA are published in the NASA X.500 Directory

- copies of the X.509 Certificate Policy for NASA PKI and this CPS are published on a web site

The NASA CA will provide a full text version of the CPS when necessary for the purposes of any audit, accreditation, or cross-certification.

2.6.2 Frequency Of Publication

Once activated, certificates issued by the NASA CA are automatically posted to the NASA X.500 Directory. When certificates are revoked they are written in CRL's which are published in accordance with section 4.4.9 of this CPS. When cross certificates are revoked they are written in ARLs that are published in accordance with section 4.4.9 of this CPS.

2.6.3 Access Controls

The NASA CA CPS and the X.509 Certificate Policy for NASA PKI have read only access and are available via the web site. Only NASA CA personnel have write or modify access on these documents.

Certificates and CRLs are available via the NASA X.500 Directory and are read only. Only the NASA CA has read/write and delete privileges.

2.6.4 Repositories

The repository for certificates, CRLs and ARLs issued by the NASA CA is provided by the NASA X.500 directory system. The protocol used to access the directory is the Lightweight Directory Access Protocol (LDAP) version 2, as specified in Request for Comment (RFC) 1777 *Lightweight Directory Access Protocol* (1995). LDAP version 2 is used over TCP transport, as defined in section 3.1 of RFC 1777.

When conveyed in LDAP requests and results, attributes defined in X.500 are encoded using string representations defined in RFC 1778 *The String Representation of Standard Attribute Syntaxes* (1995). These string encodings were based on the attribute definitions from X.500 (1988). Thus, the string representations of the following are for version 1 certificates and version 1 revocation lists:

userCertificate (RFC 1778 section 2.25)
cACertificate (RFC 1778 section 2.26)
authorityRevocationList, (RFC 1778 section 2.27)
certificateRevocationList, (RFC 1778 section 2.28)
crossCertificatePair, (RFC 1778 section 2.29)

Since this CPS uses version 3 certificates and version 2 revocation lists, as defined in X.509, the RFC 1778 string encoding of these attributes is inappropriate. For this reason, these attributes are encoded using a syntax similar to the syntax Undefined from section 2.1 of RFC 1778: values of these attributes are encoded as if they were values of type OCTET STRING, with the string value of the encoding being the DER-encoding of the value itself.

The repository for this CPS and the X.509 Certificate Policy for NASA PKI is a web site that is accessible at http://nasaca.nasa.gov.

2.7 COMPLIANCE AUDIT

2.7.1 Frequency Of Compliance Audit

A full and formal audit on the NASA CA operation is performed annually.

The NASA PA may order a compliance audit by an auditor at any time at its discretion.

The NASA CA reserves the right to require periodic and aperiodic inspections and audits of any RA facility within the NASA CA's domain to validate that the RA is operating in accordance with the security practices and procedures laid out in this CPS.

2.7.2 Identity/qualifications Of CA Auditor

The NASA PA will approve the auditor or auditing organization to be used for compliance audits. The auditor must perform CA or Information System Security Audits as its primary responsibility, demonstrate significant experience with PKI and cryptographic technologies as well as the operation of relevant PKI software.

2.7.3 Auditor’s Relationship To Audited CA

The auditor approved by the NASA PA can be contracted by NASA or can be an organization within NASA sufficiently separated from the NASA CA to provide an unbiased, independent evaluation.

2.7.4 Topics Covered By Audit

The purpose of the audit shall be to verify that the NASA CA is implementing its practices and policies in accordance with this CPS and the X.509 Certificate Policy for NASA PKI. Some areas of focus for the audit are:

- identification and authentication
- operational functions/services
- physical, procedural and personnel security controls
- technical security controls

2.7.5 Actions Taken As A Result Of Audit

Any discrepancies between the NASA CA’s operation, and the stipulations of this CPS shall be recorded by the auditor in a formal report to be submitted to the NASA PA. In addition to noting any discrepancies, the auditor will note the severity of any discrepancies.

The NASA PA in consultation with the NASA CA shall determine:

- the remedy for any noted discrepancies;
- a time for completing remedies to any discrepancies noted; and

- if other parties require notification, in relation to the type and severity of any discrepancies. In the case of discrepancies classified as severe discrepancies, which affect other parties, the affected parties will be notified of the discrepancies and the actions being taken to remedy the discrepancies.

If any discrepancies are identified in the auditor's report to the NASA PA, the NASA PA in consultation with the NASA CA will determine which of these actions to take:

1) Continue to operate as usual.
2) Continue to operate but at a lower assurance level.
3) Suspend operation.

The decision regarding which of these actions to take will be based on the severity of the discrepancy, the risks imposed, and the disruption to the certificate using community.

If Action 1 or 2 is taken, the NASA PA and the NASA PKI Operations are responsible for ensuring that corrective actions are taken within 30 days. At that time, or earlier if approved by the NASA PA and auditor, the audit team shall reassess. If, upon reassessment, corrective actions have not been taken, the auditor determines if more severe action (e.g. Action **3**) is required.

If Action 3 is taken, all certificates issued by the NASA CA, including End Entity certificates and CA cross certificates, are revoked prior to the suspension of the service.

The NASA PA and the NASA CA NASA PKI Operations are responsible for reporting the status of any corrective action to the auditor on a weekly basis. The NASA PA and auditor together determine when the re-assessment is to occur. If the discrepancies are deemed to be corrected upon reassessment, the NASA CA shall resume service and new certificates may be issued to End Entities and other external CAs, depending on conditions specified in individual cross certification agreements.

2.7.6 Communication Of Results

Results of the annual audit are provided to the NASA PA, and the NASA CA. In the case of Action 2, the NASA PA, with assistance from the auditor, determines if Subscribers need to be informed of the action. In the case of Action 3, the NASA PA ensures that all Subscribers are informed of the action. Communication with the purpose of informing Subscribers of any deficiency and action is performed via email when possible. If a Subscriber does not have email access, then a memo is delivered through the NASA mail service.

The method and detail of notification of audit results to CAs cross certified with the NASA CA shall be defined within the cross certification agreement between the two parties. Unless specified in a particular cross certification agreement, no communication of the audit results shall occur outside NASA.

2.8 CONFIDENTIALITY OF INFORMATION

All information that is not considered by the NASA PA to be public will be kept confidential.

2.8.1 Types Of Information To Be Kept Confidential

Each Subscriber's private signing key is confidential to that Subscriber. The NASA CA and RAs are not provided any access to those keys.

The Subscriber's copy of their confidentiality (i.e. encryption) private key must be kept confidential by the Subscriber. However, confidentiality private keys are backed-up by the NASA CA and are protected in accordance with section 6 of this CPS.

Information held in audit trails is considered confidential to NASA and shall not be released outside the agency, unless required by law.

Collection of personal information may be subject to collection, maintenance, retention and protection requirements of the Privacy Act of 1974, 5 U.S.C. 552a. Access to information stored locally by a CA or RA shall be restricted to those with an official need-to-know in order to perform their official duties.

Personal and corporate information held by the NASA PA, CA and RA, other than that which is explicitly published as part of a certificate, CRL, or ARL, is considered confidential and shall not be released unless required by law.

Generally, the results of annual audits are kept confidential, with exceptions as outlined in section 2.7.6 of this CPS.

In general, audit logs will not be publicly available.

Any keys held by the NASA CA are considered confidential and shall be released only to a authorized NASA organizational authority, in accordance with this CPS, and the X.509 Certificate Policy for NASA PKI, or a law enforcement official, in accordance with US law and this CPS.

2.8.2 Types Of Information Not Considered Confidential

Information included in public certificates, CRLs, and ARLs issued by the NASA CA are not considered confidential.

Information in the X.509 Certificate Policy for NASA PKI and this CPS is not considered confidential.

Confidentiality of relevant information in the directory is achieved through the use of access controls.

2.8.3 Disclosure Of Certificate Revocation Information

When a certificate is revoked by the NASA CA, a reason code is included in the CRL entry for the action. This reason code is not considered confidential and may be shared with all other Subscribers and Relying Parties. However, no other details concerning the revocation are disclosed.

2.8.4 Information Release

The NASA CA and RAs will not disclose certificate or certificate-related information to any third party, except when:

- authorized by the X.509 Certificate Policy for NASA PKI and this CPS;
- required to be disclosed by law, U.S. governmental rule or regulation, or court order;
- required to release information to law enforcement officials, consistent with the NASA agency policy; or
- authorized by the Subscriber when necessary to effect an appropriate use of the certificate.

Any requests for the disclosure of information must be signed and delivered to the local NASA RA or NASA CA.

2.8.5 Release As Part Of Civil Discovery

To release information as part of civil discovery, the NASA CA will comply with the NASA agency policy.

2.8.6 Other Information Release Circumstances

No stipulation.

2.9 INTELLECTUAL PROPERTY RIGHTS

The U.S. Government, as represented by the Administrator of the National Aeronautics and Space Administration, retains exclusive right to any product or information developed by NASA under or pursuant to this CPS including, but not limited to, any public key certificates and private keys that it issues. The rights to any product or information developed by a U.S. Government contractor under or pursuant to this CPS will be governed by the terms of the contract and U.S. federal laws and regulations. Rights in the NASA name, initials, Seal and other devices are governed by section 311 of the National Aeronautics and Space Act of 1958, as amended (42 U.S.C. 2459b) and regulations at 14 CFR Part 1221.

3. Identification & Authentication

3.1 INITIAL REGISTRATION

3.1.1 Types Of Names

Names for certificate issuers and certificate subjects are of the X.500 Distinguished Name (DN) form. The National Aeronautics and Space Administration is a registered name in accordance with ANSI, the US National Name Registration Authority. A single naming hierarchy is established within NASA as outlined below:

- Names for certificate issuers (i.e. the NASA CA) and certificate subjects (i.e. Subscriber or End Entity) are of the X.500 Distinguished Name (DN) form. These names are unique and unambiguous within the NASA hierarchy as specified in the NASA Directory Service Architecture, Standards and Products document.
- Certificate issuers have entries at the organizationName level whose DNs shall be of the form (for example): cn=NASACA, o=National Aeronautics and Space Administration, c=US.
- Certificate subjects shall have entries at the organizationalUnitName level. The DNs will follow the following form: cn=Jane Doe, ou=NASA Center name, o=National Aeronautics and Space Administration, c=US.

All attributes identified in this section are as defined in ITU-T Recommendation X.521 *Information Technology – Open Systems Interconnection – The Directory: Selected Object Classes* (1988).

Certificate subjects may choose an optional Alternated Subject Name in which case this object should be marked non-critical. Certificate subjects may choose to have additional name forms, such as an email address, however the DN is the primary name and the one used to populate the subject fields of certificates, CRLs, and ARLs.

Note that additional objects outside the scope of this CPS are present in the naming hierarchy.

3.1.2 Need For Names To Be Meaningful

If the Subscriber is an individual, the name assigned to the commonName attribute is the Subscriber’s name. If the Subscriber is an organization or a device, the name of the person responsible for that device or organization appears in the directory entry.

3.1.3 Rules For Interpreting Various Name Forms

As the NASA Center responsible for management and operation of the NASA X.500, Marshall Space Flight Center is responsible for the NASA X.500 directory name space.

3.1.4 Uniqueness Of Names

X.500 distinguished names are unique for all End Entities within the NASA CA domain. At the discretion of the NASA CA and RAs, other names, numbers, and letters may be appended to ensure the distinguished name's uniqueness within their respective X.500 name space.

3.1.5 Name Claim Dispute Resolution Procedure

No stipulation.

3.1.6 Recognition, Authentication And Roles Of Trademarks

The NASA CA and RAs authenticate names of employees and other entities within the NASA organization. Although the NASA CA shall establish cross certification with other CA domains, identified by the Distinguished Name, the naming and trademark issues associated with those names within those domains is outside the scope of this CPS.

3.1.7 Method To Prove Possession Of Private Key

The NASA CA supports RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols.

3.1.8 Authentication Of Organization Identity

Public-key certificates are issued to individuals whenever possible. For those cases where there are several individuals acting in one capacity, a certificate may be issued that contains the name of an organization.

An application for an organization must be made by an individual authorized to act on behalf of the prospective Subscriber (i.e. organization). This authorized individual must be the person in the organization who will be responsible for ensuring control of the certificates and the associated private keys, including accounting for which individual of the organization has control of the keys at what time. In addition, in the case of an organization, the confidentiality (i.e. encryption) key pair shall be used but the digital signature key pair shall not be used.

Identification and authentication of the prospective Subscriber is as follows:

- requests for organizational certificates include the organization name, address, and documentation of the existence of the organization;
- the RA or CA examines notarized copies of documentation providing evidence of the existence of the organization (for business organizations or partners outside of NASA);
- the RA or CA verifies the identity and authority of the individual acting on behalf of the prospective Subscriber and their authority to receive the keys on behalf of that organization;
- the RA or CA keeps a record of the type and details of identification used; and
- the RA or CA shall retain the name of the person to whom the organizational certificate is issued.

The procedures for issuing organizational certificates do not conflict with other stipulations of this CPS (e.g., key generation, private key protection, and Subscriber obligations).

In the case of issuing cross-certificates to other CAs, the NASA CA issues cross certificates to other CAs with the approval of the NASA PA. The NASA PA reviews the policies and procedures of the other CA before approving a cross certification. Conversely, the NASA CA's CPS and X.509 Certificate Policy for NASA PKI are made available to the other CA for review.

The NASA PA authenticates the other CA using existing business agreements between NASA and the other CA's organization or through searches of recognized databases of registered corporations, or by presentation of the organization's articles of incorporation to the NASA PA. In all cases, the authentication documentation are filed and retained by the NASA PA.

3.1.9 Authentication Of Individual Identity

An application for an individual to be a Subscriber must be made by the individual. In addition to the identification and authentication described below, the prospective Subscriber must personally present him or herself to their local RA for authentication prior to certificate issuance.

It is the responsibility of the RA to verify the identity of the Subscriber applying for a certificate. The authentication procedure includes the processes described in the following sections. The RA obtains confirmation of 1) *affiliation* with NASA and 2) *identity*.

3.1.9.1 AUTHENTICATION OF SUBSCRIBER'S AFFILIATION

Confirmation of the Subscriber's affiliation with NASA must be provided to the RA before a certificate may be issued to the Subscriber. Confirmation of the Subscriber's affiliation is through one of the following means:

1.) For most NASA personnel proof of affiliation is provided through the identification badge issued to the individual at his/her entrance-on-duty. If the badge issuing procedure provides for the assurance described below, the RA may accept the badge as confirmation of affiliation.

    For the badge to be considered confirmation of affiliation, the badge issuer must have received official notification of the individual's affiliation.
    - *For civil servants*, the badge issuer must receive notification of employment from the Center's Human Resources department. The badge issuer must retain this notification. Examples of acceptable notification include official federal employment forms or written and signed notification from the Center's Human Resources hiring officials.
    - *For contractors*, the badge issuer must receive confirmation from the contractor's Contracting Officer's Technical Representative (COTR) or Technical Monitor.

2.) For NASA Centers in which the badge process does not meet the requirement noted above, the RA receives and retains notification of the individual's affiliation. For civil servants, the RA receives written and signed confirmation from the Center's Human Resources department. For contractors, the RA receives written and signed confirmation from the contractor's COTR or Technical Monitor.

3.1.9.2 AUTHENTICATION OF SUBSCRIBER'S IDENTITY

The RA performs identity verification either at the time of the certificate request or prior to the request. The RA files and retains authentication documentation described below.

Confirmation of the Subscriber's identity must be through one of the following means:

1.) For some NASA Centers, identity checks may be performed as part of the initial hiring and badge procedure for civil servants and/or contractors. If so, a RA must either retain a copy of the form used to collect and verify the identity information (ex. NASA form 531) or show access to a database or file where the information is retained.

2.) For a NASA Center that does not provide identity checks, the RA performs the identity verification or can be shown a form of identification for which an identity check has previously been performed.

2a.) For RAs performing identity verification, the following information is obtained for identity verification as part of an identity check:

- full Name (Last, First, Middle)
- current residence (number, street, city, state and zip)
- date of birth
- place of birth
- citizenship
- social security number

If not a US citizen or a naturalized citizen, one of the following identification numbers is obtained in addition to the list above:

- alien registration number or
- US naturalization number

The RA records and retains the information checked along with the sources used to check the information.

2b.) For RAs accepting other form of identification, in addition to the NASA badge, one of the following forms of identification is accepted for identity verification, one of which must include a picture:

- passport
- birth certificate
- driver's license or state identification card
- certificate of naturalization

If not a US citizen, another form of identification must be presented *in addition* to those listed above*:*

- permanent resident card

The RA accepting other form of identification makes a copy of the form of identification accepted or records and retains the following:

- the forms of identification accepted
- any unique identification information associated with the form, such as passport number or drivers license number
- any expiration information associated with the form

3.1.10 Authentication Of Devices Or Applications

A device or application can be named as certificate subjects. In such cases, the device or application must have a human sponsor. Application must be made by an individual or organization to which the device or application is attributable.

Identification and authentication of the applicant follows section 3.1.8 or 3.1.9 as if that individual or organization were applying for the certificate on his/her own behalf.

3.2 AUTHENTICATION FOR ROUTINE REKEY

Re-keying a certificate means that that a new certificate is created that is identical to the old one, except that the new certificate has a new, different public key; a different serial number; and may be assigned a different validity period.

Only NASA employee (i.e. civil servants) key certificates are updated automatically. As such, both the encryption and digital signature key pairs are automatically updated prior to expiration. Prior to expiration of the current key pairs, the NASA CA software invokes the operation of a secure communications protocol and the Subscriber's keys are updated transparently. Authentication of the individual's identity need not be repeated.

All other entities are not provided automatic key update. These entities must identify themselves as in an initial request, in accordance with section 3.1 of this CPS.

For cross certification relationships, no automatic rekey is provided. If the NASA PA determines that a cross certification agreement is to extend beyond the original period, a new cross certificate is issued, prior to expiration of the current one. The same identification and authentication process used for initial cross certification agreements applies to the issuance of new keys.

3.3 AUTHENTICATION FOR REKEY AFTER REVOCATION

For Subscribers whose certificates have been revoked, rekey is not permitted until the identification and authentication requirements for initial registration are repeated, except in the following situations:

- an organizational change within NASA results in changes to the Distinguished Names of several employees
- a Subscriber is temporarily unable to present himself or herself in person (e.g. on extended travel) and the revocation was not due to a key compromise in which case re-key must meet the criteria for certificate issuance to geographically remote Subscribers.

For revoked cross certificates, no rekey is done.

3.4 AUTHENTICATION OF REVOCATION REQUEST

Revocation is described in section 4.4 of this CPS.

4. Operational Requirements

4.1 APPLICATION FOR A CERTIFICATE

Prior to certificate issuance, a Subscriber must submit a request. The request includes the following information:

- the Subscriber's full name
- the Subscriber's citizenship
- the Subscriber's type of NASA affiliation (civil servant or contractor)
- proof of Subscriber's affiliation
- the Subscriber's work e-mail address
- the Subscriber's work telephone number
- purpose for use of certificate
- acknowledgement of the terms specified in this CPS and Subscriber Agreement using the wording below:
  - I acknowledge and declare that, prior to applying for, accepting or using the NASA Public Key Certificate, I have read and accepted the conditions in the NASA PKI Subscriber Agreement. The NASA PKI Subscriber Agreement is available on the Internet at http://nasaca.nasa.gov/docs.html. I am aware that the X.509 Certificate Policy for NASA PKI and the NASA Certification Authority Certification Practice Statement are available on the Internet at http://nasaca.nasa.gov/docs.html and I accept the subscriber obligations and responsibilities contained therein as summarized in the NASA PKI Subscriber Agreement.

    I hereby certify that the information provided by me is true and correct to the best of my knowledge and belief.
- date and signature of civil servant or requesting contractor
- date and signature of approving authority [for contractors

Depending on the RA's authentication process, the RA may choose to include additional information on the certificate request to assist in the identity confirmation.

For civil servants, the certificate request is dated and signed by the requesting civil servant.

For contractors, the certificate request is signed and dated by the requesting contractor and the contractor's COTR or Technical Monitor. The COTR/Technical Monitor also indicates the validity period for the certificate. Depending on the RA's authentication process, the RA may require additional information from a contractor, such as the name of the Contractor for whom the requestor works, the Contract Number, the name of the COTR/Technical Monitor, the location and telephone number of the COTR/Technical Monitor.

Using the information provided by the certificate requester, the RA performs an identity verification according to the requirements noted in sections 3.1.8 or 3.1.9. Based on the verification, the RA either accepts or refuses the certificate request. The RA notifies the Subscriber of acceptance or refusal. The RA notes the action taken on the certificate request, the verification action taken and then signs and dates the request. The RA retains the certificate request.

4.2 CERTIFICATE ISSUANCE

Certificates are issued upon completion of the identity verification and the certificate application. Before the RA issues the certificate, the Subscriber must have an entry in the Center's X.500 Directory. The Center's X.500 Directory Administrator works with the RA to confirm the Subscriber's X.500 directory entry.

The RA logs in to the CA server to create a certificate for the Subscriber. The RA enables the Subscriber using the Subscriber's Distinguished Name from the X.500 Directory and records the event in the RA Administrator Logbook. The enabling operation results in the creation of authorization information that the RA securely distributes to the Subscriber. The Subscriber needs the authorization information to initially log in and complete the key and certificate generation process.

The RA contacts the Subscriber for collection of the Subscriber's authorization information. Subscribers present themselves in person to receive their authorization information. To receive the authorization information, the Subscriber presents picture identification to the RA to provide confirmation that he/she is indeed the person who requested the certificate. With this confirmation, the RA provides the Subscriber with the authorization information. The Subscriber is required to use this information within 5 working days of initial registration and agree not to divulge this information prior to their initialization.

To complete the certificate issuance process, the Subscriber installs PKI client software on his/her computer. The Subscriber logs in to the PKI client and enters the authorization information provided to him/her. A secure communication is established between the Subscriber's PKI client software and the NASA CA. The PKI client software creates the signing key pair and the NASA CA creates the encryption key pair. The NASA CA signs the signing and encryption public key certificates, stores a copy of the certificates in the NASA CA database, and returns a copy of the certificates and a copy of the private encryption key to the PKI client software. In addition, the NASA CA writes the public certificates to the NASA X.500 directory. The NASA CA stores the encryption private key in encrypted form. The PKI client software stores the encryption key pair and the signing key pair in encrypted form.

If the RA must issue certificates to Subscribers who are not in the same geographical location as the RA, the RA and the Subscriber arrange a process in which the authorization information can be securely delivered to the Subscriber and the Subscriber can confirm their identity remotely.

The issuance and publication of a certificate by the NASA CA indicates a complete and final approval of the certificate application.

For information on delivery of key pairs for certificate issuance, please refer to sections 6.1.2 and 6.1.4 of this CPS.

4.3 CERTIFICATE ACCEPTANCE

Acceptance by the Subscriber of his/her responsibilities regarding certificate use is secured in the certificate request process as described in section 4.1 of this CPS. The Subscriber signs an acknowledgement of the terms of this CPS and terms noted in the Subscriber's Agreement.

Acceptance of the certificate occurs in the certificate issuance process described in section 4.2 of this CPS. The operation of the secure communications protocol between the Subscriber and the NASA CA involves the mutual authentication of the two parties and request and response operations that constitute acceptance by the Subscriber of the resulting public key certificates.

4.4 CERTIFICATE SUSPENSION & REVOCATION

4.4.1 Circumstances For Revocation

Certificates are revoked when the certificates are no longer trusted, for any reason. This includes certificates for Subscribers, RAs, and CA Officers. Reasons for loss of trust in certificates include, but are not limited to:

- the Subscriber's employment is terminated or Subscriber is suspended for cause
- compromise or suspected compromise of private keys and/or password and profile
- change in Subscriber's role (such as organizational change between Centers) or permissions
- media holding the private key is compromised or suspected of compromise, as applicable
- failure of the Subscriber to meet their obligations under this CPS, the X.509 Certificate Policy for NASA PKI any agreement, or any applicable law
- the Subscriber or other authorized party (as defined in section 4.4.2) requests that the certificate be revoked

Cross certificate issued by the NASA CA to another CA are revoked when the certificate is no longer trusted for any reason or if the relationship is no longer required. Reasons for loss of trust in cross-certificates include, but are not limited to:

- compromise or suspected compromise of private keys
- corporate mergers or takeovers
- failure of the cross-certified CA to meet their obligations as stated in the cross certification agreement
- unexpected changes to the business relationship between the two entities

4.4.2 Who Can Request Revocation

The revocation of a certificate may only be requested by:

- the Subscriber in whose name the certificate has been issued

- the individual or organization who made the application for the certificate on behalf of a device or application
- the Subscriber's management, if the Subscriber is a NASA employee or contractor
- personnel of the NASA CA
- personnel of a RA associated with the NASA CA
- a NASA Center's Information Technology (IT) Security Manager
- the NASA PA

4.4.3 Procedure For Revocation Request

Any requester wishing to revoke a certificate, must notify their local RA, complete and sign a written request for revocation, and present themselves in person with their badge.

Written requests must be obtained for auditing purposes and must contain the following information:

- date of revocation request
- name of the owner of the certificate (i.e. Subscriber)
- certificate owner's NASA organization (if applicable)
- detailed reason for requesting revocation
- name and title of person requesting revocation
- contact information of person requesting revocation
- signature of person requesting revocation

Written requests are sent to the RA. In cases requiring immediate revocation of a Subscriber's certificate an email request or call must be sent to the RA.

Upon receipt and confirmation of the written request, the RA revokes the Subscriber's certificate by logging in to the CA server and performing the certificate revocation. The RA records the event in the RA Administration Logbook. The RA notes the action taken on the written request and then signs and dates the request. The RA retains the revocation written request. Revoked certificates shall remain on the CRL until the certificate expires.

Revocation of a certificate of a person in a RA role will follow the procedures for completing and signing a request for revocation as noted in this section. The RA not requesting revocation, will send a signed and encrypted email to the NASA CA requesting that the role of the RA requesting revocation be changed from RA to User. The NASA CA will return a signed and encrypted email confirming the role change. The NASA CA records the event in the CA Officer Logbook. The RA not requesting revocation can then complete the action by performing the certificate revocation. The RA records the event in the RA Administration Logbook. The RA notes the action taken on the written request and then signs and dates the request.

4.4.4 Revocation Request Grace Period

Key compromise, suspected key compromise, and dismissal for cause are identified as security incidents and are handled by locally defined IT security incident/response procedures at each NASA Center. Revocation requests for other revocation reasons are placed within 24 hours of the change.

4.4.5 Circumstances For Suspension

The NASA CA may disable/suspend a Subscriber's certificate if a Subscriber goes on leave. The NASA CA may disable/suspend a Subscriber's certificate in support of a security investigation by internal NASA security personnel or external law enforcement agencies. Unlike revocation, disabling a Subscriber allows for re-enabling at a later time.

Information on public keys of disabled Subscribers is not available in the NASA X.500 Directory, but it is retained in the NASA CA database. Once the certificate is disabled/suspended, the Subscriber's keys are not available for encryption or signing. However, any files that were signed prior to the suspension may be verified by recipients.

Cross certificates are not suspended.

4.4.6 Who Can Request Suspension

The parties identified in section 4.4.2 can also request disabling/suspending a certificate.

4.4.7 Procedure For Suspension Request

Any requester wishing to disable/suspend a certificate, must notify their local RA, complete and sign a written request for suspension, and present themselves in person with their badge.

Written requests are required for disable/suspension for auditing purposes and must contain the following information:

- date of suspension request
- name of the owner of the certificate (i.e. Subscriber)
- time period of suspension
- certificate owner's NASA organization (if applicable)
- detailed reason for requesting suspension
- name and title of person requesting suspension
- contact information of person requesting suspension
- signature of person requesting suspension

Written requests are sent to the RA. In cases requiring immediate suspension of a Subscriber's certificate either an email or a call may be placed to the RA.

Upon receipt and confirmation of suspension request, the RA shall suspend the Subscriber's certificate and shall record the event in the Administration Logbook. The RA must note the action taken on the written request, and then sign and date the request. The RA shall retain the written request of suspension.

Upon receipt and confirmation of the written request, the RA disables the Subscriber by logging in to the CA server and performing the disable. The RA records the event in the RA Administration Logbook. The RA notes the action taken on the written request and then signs and dates the request. The RA retains the suspension written request.

Suspension of a certificate of a person in a RA role will follow the procedures for completing and signing a request for suspension as noted in this section. The RA not requesting suspension, will send a signed and encrypted email to the NASA CA requesting that the role of the RA requesting suspension be changed from RA to User. The NASA CA will return a signed and encrypted email confirming the role change. The NASA CA records the event in the CA Officer logbook. The RA not requesting suspension can then complete the action by performing the certificate suspension. The RA records the event in the RA Administration Logbook. The RA notes the action taken on the written request and then signs and dates the request.

4.4.8 Limits On Suspension Period

The requesting party stipulates the suspension period in the suspension request.

4.4.9 CRL Issuance Frequency

The NASA CA issues CRLs and ARLs to the NASA X.500 Directory every 12 hours. The CRLs and ARLs are issued 7 days per week. Upon exception, CRLs and ARLs may also be issued *between* these intervals (e.g.: upon detection of a serious compromise situation).

4.4.10 CRL Checking Requirements

Each certificate issued by the NASA CA shall include the full DN of the CRL Distribution Point to be checked during the verification of the certificate.

Before using a certificate, Relying Parties must check its status against a current copy of the CRL. The Relying Parties PKI software should verify the CA’s signature on the CRLs and ARLs. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject the use of the certificate, or make an informed decision to accept the risk, responsibility and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this CPS.

4.4.11 On-line Revocation/status Checking Availability

The NASA PKI does not currently support on-line revocation/status checking.

4.4.12 On-line Revocation Checking Requirements

No stipulation.

4.4.13 Other Forms Of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements For Other Forms Of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Related To Key Compromise

For information on key compromise, please refer to section 4.8.3. of this CPS.

4.5 SYSTEM SECURITY AUDIT PROCEDURES

4.5.1 Types Of Event Recorded

All significant security events on the NASA CA software are automatically timestamped and recorded in audit log files. These include:

NASA CA System [application software] Events

Audit log changes

- any changes to audit log parameters such as audit frequency, types of events audited
- attempts to modify or delete the audit logs

Authentication

- successful and unsuccessful attempts to login and authenticate as a CA trusted role
- changes in rules for authentication
- maximum number of unsuccessful authentication attempts during login

Key Generation

- CA key generation actions including CA key changeover (keys used for single session are excluded)

Private Key Access

- access to private keys retained within the NASA CA for key recovery purposes
- export of private keys (keys used for single session are excluded)

Public Key Entry, and Deletion

- changes to public keys (including additions and deletions)

Certificate Management Requests and Actions

- all certificate management requests and subsequent actions to include:
- certificate creation
- certificate changes to include:
  - ➢ update
  - ➢ suspension/disable
  - ➢ recovery
- certificate revocation

Certificate Revocation List Management Actions

- all certificate revocation list actions

Directory Posting Actions

- posting of CA and certificate information to a directory

Account and Policy Administration

- addition or deletion of roles and entities
- changes to access privileges of roles or entities

- changes to the NASA CA's policies as implemented within the NASA CA's software

Other events outside the NASA CA software include:

NASA CA System and Application Administration Events

- system start-up and shutdown
- logon to the NASA's CA application software
- re-set or change to passwords
- back-up or restore of the NASA CA's application database
- access to the NASA CA's application database
- installation, removing or destruction of hardware module holding the CA signing key
- software check integrity failures
- resetting operating system clock
- changes to the NASA CA server configuration to include hardware, software, operating system and patches

NASA CA Facility Access Events

- the NASA CA facility has an electronic monitoring system that provides information concerning access to the NASA CA facility

NASA CA Support Systems Events

- the NASA CA has an Uniterruptible Power Supply (UPS) which provides information on the status of the power supply

4.5.2 Frequency Of Audit Log Processing

The NASA CA Officers process audit logs weekly, investigating any alerts or irregularities in the logs.

4.5.3 Retention Period For Audit Log

The audit trails are electronically retained indefinitely under the NASA CA configurations. Section 4.5.5 describes the retention procedures for these logs.

4.5.4 Protection Of Audit Log

The audit trail is stored in regular operating system flat files. Each audit trail file consists of an audit header that contains information about the audits in the file and a list of events. A Message Authentication Code (MAC) is created for each of the audit events and the audit header. Each audit trail file has a different audit key used to generate the MAC. The NASA CA Master User for the NASA CA protects the audit key that is stored in the audit header. The CA Officer is responsible for reviewing the audit logs. As the audit log reviewer, the CA Officer cannot modify the audit log.

The audit trail can be spread across many files. A new audit trail file is created whenever the current audit trail file reaches a preset size of 100 Kbytes or the CA master key is updated.

Audit logs are protected through the means noted above and are protected from unauthorized viewing and/or modification through restrictions via the CA server operating system and access restrictions noted in section 5.1.1 of this CPS.

4.5.5 Audit Log Backup Procedures

Audit trails are backed up nightly as part of a regular NASA CA system backup. Audit trail files are retained by the CA system administrator on a weekly basis. On a monthly basis, the files, including a full system back up, are moved to magnetic tapes and stored in a secure records retention facility.

4.5.6 Audit Collection System

The audit trail accumulation system is internal to the NASA CA software system. This information is collected via the backup procedures specified in section 4.5.5.

4.5.7 Notification To Event Causing Subject

Where an event is logged by the audit collection system, notification is not sent to the individual causing the audit event. The subject may be notified that their action was successful or unsuccessful but not that their action was audited.

4.5.8 Vulnerability Assessments

The NASA CA system administrator, and other CA operation personnel use the processes identified in the System Security Audit Procedures section of this CPS to monitor, assess and address as required system vulnerabilities.

4.5.9 RA And CA Officer Logbooks

The purpose of the RA Administration Logbook and the CA Officer Logbook are to log events so that in cases in which the CA database must be recovered, the RA logbooks and CA Officer Logbook can be used to reconstruct events not captured on the last CA database backup.

The logbooks should be hardcover with numbered pages and stitched binding. Log entries should be entered in ink. Log entries should include the date and time an action was taken, a description of the action taken, the name of the person(s) executing the action, and the signature(s) of the person(s).

The logbooks should be under the control of the respective RA and CA Officer personnel. When not in use it should be stored in a location accessible to the respective personnel. As the logbooks will be used for data recovery, the retention period of a logbook should be at least 3 months.

4.6 Records Retention

4.6.1 Types Of Data Retained

The types of data recorded and retained by the RAs are described in section 4.6.1.1. The types of data recorded and retained by the CA are described in section 4.6.1.2.

4.6.1.1 TYPES OF DATA RETAINED BY RAS

In the execution of the RA function, various documents are provided to the RA. These documents include:

- identification information
- certificate requests/approvals
- certificate suspension requests/approvals
- certificate revocation requests/approvals
- key recovery requests/ approvals

Some information provided is personal information and falls under the Privacy Act of 1974, 5 U.S.C. 552a. This information shall be stored securely in accordance with Privacy Act 1974, 5 U.S.C. 552a requirements. Access to this information shall be limited to RA personnel.

4.6.1.2 TYPES OF DATA RETAINED BY THE NASA CA

The types of data retained include:

- confidentiality (i.e. encryption) private keys and certificates in the NASA CA database (private signing keys are not backed up)
- audit information as noted in section 4.5.1
- certificate requests/approvals as noted in section 4.6.1.1
- identification and authentication information submitted by Subscribers as noted in section 4.6.1.1
- the NASA Certification Authority Certification Practice Statement
- the NASA CA system and equipment configuration and modifications to the NASA CA system and configuration
- documentation required for compliance audits
- as performed, record of NASA CA re-key
- as applicable contractual agreements

4.6.2 Period For Record Retention

Information identified in sections 4.6.1.1 and 4.6.1.2 are preserved, maintained, and disposed of in accordance with NASA Records Retention and Schedules, NPG 1441.

4.6.3 Protection Of Record Retention

The NASA CA system database is encrypted and protected by the CA system. Protection of the audit trail is as described in section 4.5.4 of this CPS.

The record retention media is secured such that access is restricted to only CA Master Users and CA Officers. The record retention media is stored in a location with temperature, humidity and magnetism controls adequate to protect the record retention media.

4.6.4 Record Retention Backup Procedures

No stipulation

4.6.5 Time-Stamping of Records

No stipulation

4.6.6 Record Retention Collection System

The record retention collection system for the NASA CA system database is internal to the NASA CA system.

The record retention collection system for the audit trail files is described in sections 4.5.5 and 4.5.6 of this CPS.

The retention of these data onto media and the secure storage of that media are external from the NASA CA system. Packaging and storage of the media is described in section 4.5.5.

4.6.7 Procedures To Obtain And Verify Retained Information

Twice per year, the record retention media are retrieved by the CA Officer and verified to ensure no damage or loss of data has occurred. If any has occurred, the backup is retrieved, becomes the new master, and a new backup is produced.

Once every five years, a new backup is produced, even if there is no evidence of damage or loss of data on the master or backup. For each media, the new backup becomes the master, the previous master becomes the backup and the previous backup media is securely recycled.

The contents of the record retention for the NASA CA shall not be released except as determined by the NASA PA and in accordance with the NASA Records Retention and Schedules, NPG 1441.

4.7 KEY CHANGEOVER

Refer to sections 3.2 and 3.3 of this CPS, for Subscriber key changeover.

4.7.1 CA Key Changeover

A changeover of the NASA CA signing key pair can occur for the following events:

- change in the type or strength of the algorithm used by the NASA CA to sign certificates
- change the lifetimes of the NASA CA keys
- the NASA CA certificate lifetime has expired

In a NASA CA key changeover, the new NASA CA public key certificate is signed by the old NASA CA signing key, and the old NASA CA public key certificate is signed by the new NASA CA signing key. This cross-signing of certificates produces two new certificates, called link certificates. The link certificates provide a connection between the previous and the new NASA CA certificates.

4.8 Compromise and Disaster Recovery

4.8.1 Computing Resources, Software, And/or Data Are Corrupted

In the event of a disaster the NASA PKI Disaster Recovery Plan will be followed.

Refer to section 4.8.3 concerning NASA CA key compromise.

4.8.2 Entity Key Recovery

The key recovery process disables a Subscriber's current key pairs and allows for the revision of profile data by any person in possession of the newly generated authorization information. Re-initialization then allows access to a Subscriber's previously encrypted files.

Only local RAs perform key recoveries. Two RAs are present to authorize and perform key recovery operations. If two RAs are unavailable, CA Officers act as substitute administrators in emergency cases.

The timeframe for completion of non-emergency key recovery requests is within 48 hours. In emergency cases, the local RA is contacted.

4.8.2.1 Key Recovery Requested By The Subscriber

Examples of reasons for Subscriber requested key recovery include:

- a Subscriber forgets a password
- a Subscriber loses or damages a PKI profile file
- a Subscriber loses or damages a security token (PCMCIA card)
- a Subscriber suspects his/her keys have been compromised

For the Subscriber's protection from unauthorized requests, the Subscriber must a) make arrangements to appear in person and b) submit written approval to the RA stating the reason for the recovery.

Upon receipt of written approval, the RAs visually verify the identity of the Subscriber using the employee badge, and performs the key recovery process. RAs log the recovery event for auditing purposes. The RAs note the action taken on the written approval, and then sign and date the approval. The RAs retains the recovery written approval.

RAs then present the Subscriber with instructions for obtaining new authorization information.

If a Subscriber is temporarily unable to present himself or herself in person (e.g. on extended travel) and the recovery is due to forgotten password or a damaged profile file, recovery must meet the criteria for certificate issuance to geographically remote Subscribers.

4.8.2.2 KEY RECOVERY WITHOUT SUBSCRIBER CONSENT

Examples of reasons for key recovery without Subscriber consent include:

- a Subscriber has left the organization and the Subscriber's supervisor or department management needs to decrypt files for business continuity
- a Subscriber's actions are in question by the Center's IT Security Manager and the Subscriber's files need to be reviewed
- a Subscriber's actions are in question by an external law enforcement agency and the Subscriber's files need to be reviewed.

In cases in which Subscribers are not aware of a key recovery operation, Subscribers shall not be able to log into the NASA CA system with their previous password. This will alert them that their accessibility has changed. Requesters have the responsibility to assess the impact of disclosure and upon doing so, may choose not to perform a key recovery.

When Subscribers discover that they can no longer access the their keys, they most likely will contact the RA for assistance. Based on instructions from the requester, the RA disseminates information to Subscribers accordingly.

The key recovery requester needs to contact their local Center IT Security Manager. Written approval from both the Subscriber's management and from the Center IT Security Manager requesting key recovery action is submitted to the RAs before the action is performed. The request must contain the following:

- date of recovery request
- name of the owner of the keys (i.e. Subscriber)
- keys owner's NASA organization (if applicable)
- requester's name and NASA organization
- detailed reason for requesting access to Subscriber's files
- specific name(s) of person(s) allowed to see Subscriber's files and to be responsible for subsequent viewing by any unnamed persons
- description (and/or filename(s)) of Subscriber's files to be viewed, *or* statement of approval to access all files.
- description of RA's role beyond key recovery action, including what information to provide if the Subscriber should inquire about the change in their NASA CA accessibility
- NASA Center IT Security Manager and the employee's management position titles signatures, and dates of signatures.

Written approvals are sent to the RAs. Upon receipt, the RAs contact the appropriate parties to schedule key recovery actions.

Note: In certain situations, RAs may be given a court order requesting key recovery. In this case, the court order will be the equivalent of a written approval.

If applicable, requesters should bring a diskette containing Subscriber's files to be viewed at the scheduled recovery process. RAs may load files on a local machine for decrypting/viewing and then delete decrypted files at the completion of the process, avoiding potential unauthorized viewing.

Requesters should first confirm that the RAs have machines with the required software to view the files. If not, the RAs may travel to the requester's location within the NASA site.

Upon receipt of written approval, the RAs visually verify the identity of authorized person(s) using the employee badge, perform the key recovery process, and log the recovery event. The RAs note the action taken on the written approval, and then sign and date the approval. The RAs retain the written approval for auditing purposes.

If the Subscriber will be retaining accessibility privileges to the NASA CA after the requested key recovery is completed, the RAs perform another key recovery process so the Subscriber may be ensured that no one has access to their key data any longer.

When applicable, the RAs may disable the recovered Subscriber's NASA CA account after the scheduled process if a short, remote viewing time limit has been requested. Re-enabling the account shall be based on instructions provided by the requester.

4.8.2.3 KEY RECOVERY FOR RA

CA Officers perform key recoveries for RAs. Two CA Officers are present to authorize and perform key recovery operations.

The timeframe for completion of non-emergency key recovery requests is within 48 hours. Centers should indicate in their correspondence with the NASA CA if an emergency recovery is required.

The NASA CA will maintain "shared secrets" for each RA. These secrets will not be sensitive in nature (such as driver's license, social security number, etc.) but should be something known only to the individual. This database will be maintained in a secure manner. This database will be used to verify the identity of the RA prior to recovery.

When a RA needs to be recovered, the following steps will be followed:

The RA request for recovery will be forwarded to the NASA CA from the Ames Information Technology Support Center.

The RA will complete a request for recovery and fax it to the NASA CA or in the case of an electronic form, email the form to the NASA CA.

When the form is received the NASA CA Officer will contact the RA and prompt the RA for two of the supplied shared secrets chosen randomly from the database.

After receiving the correct responses from the RA, the NASA CA Officers recover the RA, records the action in the CA Officer logbook. The CA Officer notes the action taken on the form, signs and dates the form, and retains the recovery form.

4.8.2.4 KEY RECOVERY REQUESTED BY EXTERNAL ENTITY

External entities refer to any law enforcement agency (FBI, DEA, State Police, etc). Requests by an external entity must be processed through the NASA Center's IT Security Manager.

The steps in section 4.8.2.2 are followed for external entity requests.

4.8.3 Entity Key Compromise

In any key compromise situation involving an End Entity's keys, a report is filed with the local RA indicating the circumstances under which the compromise occurred. If accidental, on the part of the requester, no further action is required. Otherwise, the local RA reports the compromise to their NASA Center's Computer Security Office for a possible follow-up investigation and potential action in accordance with NASA Computer Security policies.

In the event of the compromise, or suspected compromise, of the NASA CA signing key, the NASA CA shall immediately notify the NASA PA. In conjunction with the NASA PA, the NASA CA will notify Subscribers in a means mutually agreed between the NASA PA and NASA CA, for example, notification via email. With cooperation of the NASA PA, the NASA CA shall notify all CAs to whom it has issued cross certificates via a process mutually agreed by the cross-certified CAs.

4.8.4 Disaster Recovery

In the event of a disaster or serious compromise the NASA CA will follow the NASA PKI Disaster Recovery Plan.

4.9 CA TERMINATION

In the event of NASA CA termination, the NASA PA provides oversight of the termination process. All CAs with which cross certification agreements are current at the time of cessation shall be informed so that cross certificates to the NASA CA may be revoked. The RAs shall work with the NASA CA to notify all Subscribers of the NASA CA cessation of operation.

All certificates issued by the NASA CA shall be revoked.

The NASA CA records retention shall be retained in the manner and for the time period indicated in section 4.6.2 of this CPS.

5. Physical, Procedural & Personnel Security

5.1 Physical Controls

5.1.1 Site Location And Construction

The NASA CA is contained in an area to which access is controlled through an entry point and limited to authorized personnel. The facility that houses is locked, and electronically monitored 24 hours a day and 7 days a week. Electronic logs of physical access to the NASA CA facility are maintained and reviewed.

5.1.2 Physical Access

The NASA CA facility is locked and only authorized personnel are allowed access.
The RA systems are placed in locations where access is restricted. The RA computer system is secured so to prevent anyone from removing or installing components when the system is left unattended. If the system is a desktop/tower, it is locked with a cable onto a wall or desk. If the system a laptop, it is locked away when not in use. The RAs have secure containers to store keys and documents.

Subscribers must comply with this CPS and the X.509 Certificate Policy for NASA PKI regarding protection and use of their keys. Subscribers are advised of these requirements but are not audited or monitored on a regular basis.

5.1.3 Power And Air Conditioning

The NASA CA facility is supplied with power and air conditioning sufficient to create a reliable operating environment. In addition, back-up capability is provided for operation up to 6 hours allowing for continued operation and if required an orderly shutdown of application and system actions.

5.1.4 Water Exposures

The NASA CA workstation it is not in danger of exposure to water.

5.1.5 Fire Prevention And Protection

The NASA CA facility is supplied with a fire extinguishing system in accordance with NASA Center policy and code.

5.1.6 Media Storage

Media used by the NASA CA is stored in a climate controlled environment to protect media from damage due to extremes of temperature, humidity and electro- magnetic exposure.

5.1.7 Waste Disposal

Media used for the storage of information of NASA CA files is sanitized or destroyed before released for disposal.

Normal office waste shall be removed or destroyed in accordance with local NASA Center policy.

5.1.8 Off-site Backup

The backup CA facility has equivalent security and controls as the primary NASA CA.

Information concerning NASA CA system backup is described in section 4.5.5 of this CPS.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be diligent and trustworthy as described in the next section. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

The CA and RA roles are deemed to be positions of "Public Trust" per the Office of Personnel Management (OPM) 5 CFR Parts 731, 732, and 736. Personnel filling these roles shall successfully complete investigations for Public Trust positions. Background investigation criteria and other personnel security controls are noted in the following sections.

5.2.1.1 CA TRUSTED ROLES

To ensure the one person acting alone cannot circumvent safeguards, multiple roles and individuals share responsibilities of the NASA CA. Each account on the NASA CA system has limited capabilities commensurate with the individual's role. The roles within the NASA CA are:

- CA Master Users
  Three individuals shall be assigned as CA Master Users. Master Users have the authority to:
  - ➢ maintain the NASA CA system services and the NASA CA system database; and
  - ➢ recover CA Officers in the event they have forgotten their passwords.

- CA Officers
  Three individuals are assigned as CA Officers. The CA Officers have the authority to:
  - ➢ set and modify the security policy for the NASA CA, in accordance with this CPS and the X.509 Certificate Policy for NASA PKI ;
  - ➢ set the number of required authorizations for sensitive operations;
  - ➢ add and delete other CA Officers, and RAs;

  - issue, update, and revoke cross certification agreements at the direction of the NASA PA;
  - change CA Officer and RA password rules;
  - set default certificate lifetimes;
  - oversee NASA CA system audit log retention; and
  - verify NASA CA audit logs

- CA System Administrators
  Two individuals are assigned CA system administrator responsibilities, with one acting as a backup. The CA system administrators are responsible for
  - maintaining the correct operation and configuration of the underlying hardware and software for the NASA CA; and
  - performing backups of the NASA CA system.

The procedure manuals for these roles are the NASA PKI Master User Operations Manual, the NASA PKI CA Officer Operations Manuals, and the NASA PKI CA System Administrator Manual.

5.2.1.2 RA Trusted Roles

At least two individuals at each Center are designated as RAs. RA's have the authority to:

- accept and process certificate issuance, certificate change, certificate revocation/suspension and key recovery requests
- verify of an applicant's identity
- transmit applicant information to the CA
- receive and distribute Subscriber authorization information

The procedure manual for this role is the NASA PKI Registration Authority (RA) Operations Manual.

5.2.2 Number Of Persons Required Per Task

The following tasks are defined as sensitive and require at least two individuals to perform the tasks. These individuals use a split knowledge technique of two password entry and verification to perform any sensitive operation.

Two CA Officers are required to:

- add and delete other CA Officers and RAs
- set default certificate lifetimes; and
- cross certify with other CAs.

Two RAs are required to:

- perform key recovery

5.2.3 Identification & Authentication For Each Role

Identification and authorization for CA and RA personnel follow requirements identified in sections 5.3, 5.3.1 and 5.3.2.

Once these personnel are authorized, they are issued a certificate and PKI client software, which identifies and authenticates them to the NASA CA system. In addition, they are entered in the NASA CA database with their role and authorities specified. In the execution of sensitive operations, CA and RA personnel authenticate themselves using robust password procedures.

5.3 PERSONNEL SECURITY CONTROLS

The staff responsible for operating the NASA CA is NASA PKI Operations within the Applied Information Technology Division at NASA Ames Research Center.

NASA PKI Operations and RA personnel are not to be assigned duties that cause a conflict of interest with their NASA PKI Operations and RA duties. NASA PKI Operations and RA personnel will be appointed by approving authorities at NASA Centers. Training requirements for NASA PKI Operations and RA personnel are described in section 5.3.3.

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

CA Master Users, CA Officers, and RAs are deemed to be Public Trust positions and shall successfully complete background investigations for Public Trust positions.

5.3.2 Background Check Procedures

All background checks are performed in accordance with NASA Personnel Security Policies.

5.3.3 Training Requirements

Personnel performing duties with respect to the operation of the NASA CA or RA receive:

- training in the operation of the software and/or hardware used in the NASA CA system
- training in the duties they are expected to perform
- briefing on stipulations of this CPS and the X.509 Certificate Policy for NASA PKI

The NASA PKI Operations personnel will receive orientation in the NASA CA's business resumption and disaster recovery plan procedures.

5.3.4 Retraining Frequency And Requirements

The requirements of section 5.3.3 are kept current to accommodate changes in the NASA CA system. Refresher training is conducted in accordance with these changes.

5.3.5 Job Rotation

No stipulation.

5.3.6 Sanctions For Unauthorized Actions

NASA PKI Operations or RA personnel that operates in violation of the policies and procedures stated herein may have their access to the NASA CA system revoked and may be subject to administrative discipline and possible criminal prosecution.

Repeated or significant violations of this CPS or the X.509 Certificate Policy for NASA PKI by the NASA PKI Operations or RAs may result in revocation of the NASA PKI Operations or RA personnel public key certificates.

5.3.7 Contracting Personnel

Contractor personnel employed to operate any part of the NASA CA or RAs are subject to the same criteria as a US Government employee, and cleared to the level specified in section 5.3.1.

5.3.8 Documentation Supplied To Personnel

This CPS and the X.509 Certificate Policy for NASA PKI are made available to the NASA CA and RA personnel and to Subscribers. Operation manuals are made available to CA and RA personnel so they can operate and maintain the hardware and PKI software.

In addition to the CPS and X.509 Certificate Policy for NASA PKI the Subscribers are provided information on the use and protection of the software used within the NASA domain.

6. Technical Security Controls

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

The NASA CA signing key pair is created during the initial start up of the CA master control application and is protected by the CA master key.

For Subscribers, the encryption key pair and the corresponding encryption certificate are created by the NASA CA system. For Subscribers, the PKI client software generates the digital signature key pair. Keys generated by software may be stored in a file on a disk or on a removable diskette.

The software key generation process complies with FIPS 140-1 level 1.

6.1.2 Private Key Delivery To Entity

The private decryption key is provided securely to the Subscriber via a secure communications protocol between the NASA CA system and the Subscriber's software. The authorization information is used to derive a Message Authentication Code (MAC) key that is then used to provide authentication and integrity protection for the session. For the digital signature key pair, as the key pair is generated by the Subscriber's software, no delivery of the private key is required.

For cross certificates, as the CA signing key pair is generated by the subject CA, no delivery of the signing key to the subject CA is required.

6.1.3 Public Key Delivery To Certificate Issuer

For Subscribers, as the encryption key pair is created by the NASA CA system, no delivery of the encryption public key to the certificate issuer is required. The verification public key is delivered securely to the NASA CA system using a secure communications protocol.

For cross certificates, the CA public key is provided securely from the issuing CA using a secure communications protocol. Authenticity and integrity protection are based on the authorization information.

6.1.4 CA Public Key Delivery To Users

The NASA CA public key is delivered to Subscribers in a CA certificate using a secure communications protocol. Authenticity and integrity protection is based on a MAC key derived from the authorization information.

6.1.5 Asymmetric Key Sizes

Subscribers signing key pairs are 1024 bit RSA or DSA with Secure Hash Algorithm version 1 (SHA-1) or better. Subscriber encryption key pairs are 1024 bit RSA.

The NASA CA signing key pair is 1024 bit RSA.

6.1.6 Public Key Parameters Generation

Public key parameters for DSA shall be generated in accordance with FIPS 186-2.

6.1.7 Parameter Quality Checking

Parameters for DSA shall be checked as specified in FIPS 186-2.

6.1.8 Hardware/software Key Generation

The NASA CA signing key is stored in hardware of FIPS 140-1 level 3 compliance. All other Entity keys are generated in the PKI client software. This software complies with FIPS 140-1 level 1.

6.1.9 Key Usage Purposes (as per X.509v3 field)

The digital signature key pair is used to provide authentication, integrity, and support for non-repudiation services. The encryption key pair is used to protect a symmetric key used to encrypt data and as such provides confidentiality services. The NASA CA signing key is used to sign certificates, CRLs, and ARLs issued by that CA. The session keys of the secure communications protocol are used to provide secure communications for key management operations.

6.2 PRIVATE KEY PROTECTION

The following sections describe the technical and procedural techniques for private key protection. The protections noted below do not negate the Subscriber’s responsibility to protect their private keys from disclosure. Subscribers must not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered). Subscriber’s private keys are secured through cryptographic mechanisms. For added security the Subscriber should store their private keys on a removable diskette and store the diskette in a locked drawer when not needed.

The NASA CA signing key is protected from by a combination of cryptographic software and hardware mechanisms.

6.2.1 Standards For Cryptographic- module

The cryptographic module used by the software used in the NASA CA domain complies with FIPS 140-1 level 1.

The hardware device that holds the NASA CA signing key complies with FIPS 140-1 level 3.

6.2.2 Private Key Multi-person Control

Multiple person control is required for private key recovery, refer to section 5.2.2.

6.2.3 Private Key Escrow

Escrow of private keys by an external third party is not provided.

6.2.4 Private Key Backup

The Subscriber encryption and decryption keys are backed up in the NASA CA system database. The Subscriber's private signing key is never backed up in the NASA CA system, in order to provide support for non-repudiation services. The NASA CA system database is encrypted. The NASA CA system database is backed up nightly.

A copy of the NASA CA signing key is kept at the NASA CA backup location.

6.2.5 Private Key Retention

Refer to section 4.6 of this CPS for information on key retention.

6.2.6 Private Key Entry Into Cryptographic Module

The Subscriber signing key is generated in software, within the cryptographic module, and not entered by other entities into that module.

Subscriber decryption private keys come from the NASA CA system, in an encrypted format, and are entered into the cryptographic module encrypted. Private keys are stored encrypted in the cryptographic module and are decrypted only at the time at which they are actually being used.

The initial NASA CA signing key was generated in software, within the cryptographic module, and not entered by other entities into that module. When the FIPS 140-1 level 3 hardware device was available, the key was securely transferred and stored in the hardware device. All subsequent signing keys will be generated and stored in hardware.

6.2.7 Method Of Activating Private Key

Subscriber private keys are activated upon completion of login to the PKI client software. The login is in the form of a password that is protected from disclosure while it is being entered.

The NASA CA signing key is activated when the CA server is brought up and the Master User logs into the hardware device. The login is in the form of a password that is protected from disclosure while it is being entered.

6.2.8 Method Of Deactivating Private Key

The private keys remain active for the period of login. The login period is ended either by the Subscriber logging out or automatically as determined by a preset timer. The timer uses a default of 15 minutes as the maximum time allowed before automatic logout.

Subscriber private keys are always zeroized from memory when deactivated. Keys are always encrypted while in long term storage.

The NASA CA signing key is deactivated when the CA server is brought down or shut down and the Master User logs out of the hardware device. The CA signing keys remains securely stored within the hardware device when deactivated.

6.2.9 Method Of Destroying Private Key

All sensitive keys in memory are overwritten with zeros when no longer used. Permanent destruction of private keys is achieved with secure delete operations.

At this time, Subscribers keys are not held on tokens, therefore there are no destruction of physical devices.

The NASA CA signing key is held on a hardware device. If required, the CA signing key would be destroyed using zeroization as specified for FIPS 140-1 Level 3 compliant devices.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Retention

Refer to sections 6.2.4 and 6.2.5 for key backup and retention.

6.3.2 Usage Periods For The Public And Private Keys

The NASA CA public key and certificate - 20 years
The NASA CA private signing key - 20 years
Subscriber public key and certificate - two years
Subscriber private key (i.e. signing key) - 70% of public key certificate

6.4 Activation Data

6.4.1 Activation Data Generation And Installation

Passwords are required by all entities logging on to the PKI software. The software applies a stringent set of rules to each password to ensure it is secure. Rules for passwords conform to the NASA Procedures and Guidelines (NPG) 2810.1 Security of Information Technology, section A.6.3.1. [NPG 2810.1, section A6.3.1, which provides equivalent guidelines to the guidelines in FIPS 112 Password Usage]. An entity can change their password at any time.

Data used for Subscriber initialization is described in section 4.2 of this CPS.

6.4.2 Activation Data Protection

Once a Subscriber chooses a password, it is put through numerous hashing iterations, producing a password token. Only the password token is stored in a Subscriber's profile. Original passwords are never stored.

The NASA CA Server System Administration, CA Officers, and RAs, Subscriber names and password check values are stored in the NASA CA system database.

Temporary application termination occurs after a predetermined number of login attempts.

Passwords shall never be shared.

6.4.3 Other Aspects Of Activation Data

Usage periods for passwords shall be in accordance with the NASA NPG 2810.1 Security of Information Technology.

The NASA CA activation data will follow the rules specified in section 6.4.1 of this CPS and will follow usage periods in accordance with the NASA NPG 2810.1 Security of Information Technology.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The NASA CA system provides the following functionality through the operating system and a combination of the operating system, the NASA CA software and physical controls:

- access control to CA services and PKI roles;
- enforced separation of duties for PKI roles;
- identification and authentication of PKI roles and associated identities;
- use of cryptography for session communication and database security;
- retention of CA and End Entity history and audit data;
- audit of security related events; and
- recovery mechanisms for keys and the CA system.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

The NASA CA life-cycle security controls follow the guidelines specified in the NASA Procedures and Guidelines (NPG): 2810.1: Security of Information Technology.

The security management controls for the NASA CA include

- a mechanism and/or policies in place to control and monitor the CA system configuration;
- the NASA CA equipment is dedicated to administering a key management infrastructure;
- the NASA CA equipment does not have installed applications or component software, which are not part of the CA configuration, with the exception of virus protection software; and
- the NASA CA equipment updates are installed by trusted and trained personnel in a defined manner.

6.7 NETWORK SECURITY CONTROLS

Remote access to NASA CA system is secured using a secure communications protocol. No other remote access is permitted and features including inbound FTP are disabled. All TCP/IP ports are be blocked except those required by the PKI enabled event auditing and the audit of all failed operations and low-frequency successes.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

The cryptographic module of the PKI client software is designed to comply with FIPS 140-1 level 1. The NASA CA signing key is stored in a hardware device that complies with FIPS 140-1 level 3. Optional hardware tokens, which may be used to generate keys, may comply with higher levels of FIPS validation.

The cryptographic module to generate keys used by the PKI software is designed to comply with FIPS 140-1 level 1.

7. Certificate & CRL Profiles

7.1 CERTIFICATE PROFILE

7.1.1 Version Number

The NASA CA issues X.509 Version 3 certificates in accordance with the X.509 standard and IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile. The following X.509 fields are supported:

version:	version field is set to v3
serial number:	when a new user certificate is created, a unique serial number within the NASA CA security domain is generated by the NASA CA system
signature:	identifier for the algorithm used by the NASA CA to sign the certificate
issuer:	certificate issuer the NASA CA Distinguished Name
validity:	certificate validity period - notBefore start date and notAfter end date are specified
subject:	certificate subject Distinguished Name
subject public key information:	algorithm identifier (FIPS approved algorithm)

7.1.2 Certificate Extensions

A number of X.509 version 3 certificate extensions are included in certificates issued by the NASA CA. Section 7.1.2.1 describes the X.509 version 3 certificate extensions, which are supported by the NASA CA. Section 7.1.2.2 describes the X.509 version 3 certificate extensions, which are **not** present in certificates issued by the NASA CA.

7.1.2.1 SUPPORTED EXTENSIONS

The following table shows certificate extensions that are supported by the NASA CA.

X.509 v3 CERTIFICATE EXTENSION	CRITICAL/ NON CRITICAL	OPTIONAL	NOTES
SubjectAltName	Non critical	Optional	• GeneralName – The current CA system supports choices of [0], [1], [3], and [5] of General Name.
PrivateKeyUsagePeriod	Non critical	Not optional	notAfter is always used notBefore is not used
AuthorityKeyIdentifier	Non critical	Not optional	• only element [0] (authorityKeyIdentifier) is filled in • contains a 20 byte hash of the subjectPublicKeyInfo in the CA certificate
SubjectKeyIdentifier	Non critical	Not optional	contains a 20 byte hash of the subjectPublicKeyInfo in the certificate
BasicConstraints	Non critical	Not	only the cA Boolean is used

		optional	
CRLDistributionPoints	*t.b.s.*	Not optional	• only 1 distribution point name is included in each certificate • only element [0] (distributionPoint) is used and includes the full DN
KeyUsage	Non critical	Not optional	
CertificatePolicies	Non critical	Not optional	• only policyIdentifier element is supported with up to 10 OIDs • policyQualifiers not supported

The SubjectAltName field contains one or more alternative names, using any of a variety of name forms, for the entity that is bound by the NASA CA to the certified public key. This field is defined as follows:

```
 subjectAltName EXTENSION ::= {
        SYNTAX          GeneralNames
        IDENTIFIED BY id-ce-subjectAltName }

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
        OtherName                       [0]   INSTANCE OF OTHER-NAME,
        rfc822Name                      [1]   IA5String,
        dNSName                         [2]   IA5String,
        x400Address                     [3]   ORAddress,
        directoryName                   [4]   Name,
        ediPartyName                    [5]   EDIPartyName,
        uniformResourceIdentifier       [6]   IA5String,
        iPAddress                       [7]   OCTET STRING,
        registeredID                    [8]   OBJECT IDENTIFIER }
```

7.1.2.2 UNSUPPORTED EXTENSIONS

The following X.509 version 3 certificate extensions are not supported by the NASA CA:

- name constraints
- policy constraints

7.1.3 Algorithm Object IDs

The NASA CA supports the following algorithms:

Algorithm	Object Identifier	Issuing Authority
DSA-with-SHA1	1 3 14 3 2 27	OIW Security SIG
SHA1WithRSAEncryption	1 2 840 113549 1 1 5	RSADSI
DES-EDE3-CBC	1 2 840 113549 3 7	RSADSI

7.1.4 Name Forms

In a certificate, the issuer DN and subject DN fields contain the full X.500 Distinguished Name of the certificate issuer or certificate subject. If the subjectAltName extension is present in a certificate, it contains the certificate subject's rfc822Name or iPAddress with an optional email address.

7.1.5 Name Constraints

Name constraints are not used by the NASA CA.

7.1.6 Certificate Policy Object Identifier

Upon identification by the NASA PA, certificates issued under this CPS shall assert the Policy OID appropriate to the level of assurance specified in the X.509 Certificate Policy for NASA PKI and this CPS.

7.1.7 Usage Of Policy Constraints Extension

Policy constraints are not used by the NASA CA.

7.1.8 Policy Qualifiers Syntax And Semantics

No stipulation.

7.1.9 Processing Semantics For The Critical Certificate Policy

The only certificate extension, which may be identified as critical in certificates issued by the NASA CA, is the cRLDistributionPoints extension. The CRL or ARL shall be retrieved from the CRL distribution point directory entry indicated in the certificate, unless a current copy of that CRL or ARL is cached at the Subscriber's PKI client software.

7.2 CRL PROFILE

7.2.1 Version Number

CRLs issued by the NASA CA are X.509 version 2 CRLs in accordance with IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

The following is a list of the fields in the X.509 version 2 CRL format that are used by the NASA CA:

version	set to v2
signature	identifier of the algorithm used to sign the CRL
issuer	the full Distinguished Name of the NASA CA
this update	time of CRL issue
next update	time of next expected CRL update
revoked certificates	list of revoked certificate information

7.2.2 CRL and CRL Entry Extensions

Section 7.2.2.1 describers the X.509 version 2 CRL and CRL entry extensions that are supported by the NASA CA. Section 7.2.2.2 describes the X.509 version 2 CRL and CRL entry extensions that are not supported in CRLs issued by the NASA CA.

7.2.2.1 SUPPORTED EXTENSIONS

The following table the CRL and CRL entry extensions supported by the NASA CA.

X.509 v2 CRL EXTENSION	CRITICAL / NON CRITICAL	OPTIONAL	NOTES
AuthorityKeyIdentifier	Non critical	Not optional	• only element [0] (authorityKeyIdentifier) is filled in • contains a 20 byte hash of the subjectPublicKeyInfo in the CA certificate
CRLNumber	Non critical	Not optional	Incremented each time a particular CRL/ARL is changed
ReasonCode	Non critical	Not optional	CRL entry extension - only reason codes (0), (1), (3), (4) and (5) are currently supported
IssuingDistributionPoint	Critical	Not optional	• element [0] (distributionPoint) includes the full DN of the distribution point • element [1] (onlyContainsUserCerts) is included for CRLs • element [2] (onlyContainsCACerts) is included for ARLs • element [1] and [2] are never present together in the same revocation list • elements [3] and [4] are not used

7.2.2.2 UNSUPPORTED EXTENSIONS

The following X.509 version 2 CRL extensions are not supported by the NASA CA:

- issuer alternative name
- hold instruction code
- invalidity date
- certificate issuer
- delta CRL indicator

8. Specification Administration

8.1 SPECIFICATION CHANGE PROCEDURES

This CPS shall be reviewed in its entirety every year by NASA PKI Operations. Errors, updates, or suggested changes to this CPS shall be communicated to the contact in section 1.4.

8.1.1 Items That Can Change Without Notification

Changes to items within this CPS which, in the judgement of the NASA PA, have no or minimal impact on the Subscribers and cross certified CA domains using certificates and CRLs issued under this CPS, may be made with no change to the document version number and no notification to the Subscribers.

8.1.2 Changes With Notification

Changes to the certificate policy supported by this CPS as well as changes to items within this CPS which, in the judgement of the NASA PA may have significant impact on the Subscribers and cross certified CA domains using certificates and CRLs issued under this CPS, may be made with 30 days notice to the Subscribers and the version number of this CPS shall be increased accordingly.

8.1.2.1 LIST OF ITEMS

Any items in this CPS may be subject to the notification requirement as identified in sections 8.1.1 and 8.1.2.

8.1.2.2 NOTIFICATION MECHANISM

Thirty days prior to major changes to this CPS, notification of the upcoming changes will be posted on the NASA CA web site and conveyed to cross-certified CA organizations via secure email. The notification shall contain a statement of proposed changes, the final date for receipt of comments and the proposed effective date of change. The NASA PA may request CAs to notify their Subscribers of the proposed changes.

8.1.2.3 COMMENT PERIOD

The comment period will be 30 days unless otherwise specified. The comment period will be defined in the notification.

8.1.2.4 MECHANISM TO HANDLE COMMENTS

Comments on proposed changes must be directed to the Chairperson of the NASA PKI Operations. Such communication must include a description of the change, a change justification, contact information for the person requesting the change, and signature of the person requesting the change.

The NASA PKI Operations shall accept, accept with modifications, or reject the proposed change after completion of the comment period. NASA PKI operations disposition of proposed changes are reviewed with the NASA PA. Decisions with respect to the proposed changes are at the discretion of the NASA PKI Operations and the NASA PA.

8.1.2.5 PERIOD FOR FINAL CHANGE NOTICE

The NASA PKI Operations determines the period for final change notice.

8.1.2.6 ITEMS WHOSE CHANGE REQUIRES A NEW POLICY

If a policy change is determined by the NASA PA to warrant the issuance of a new policy, the NASA PA may assign a new Object Identifier (OID) for the modified policy.

8.2 PUBLICATION & NOTIFICATION PROCEDURES

NASA PKI Operations will publish this CPS and the X.509 Certificate Policy for NASA PKI on the NASA CA web site. This CPS is published at URL http://nasaca.nasa.gov. It will also disseminate information via email to any inquiries.

8.3 CPS APPROVAL PROCEDURES

The NASA PA makes the determination that the NASA CA's CPS complies with X.509 Certificate Policy for NASA PKI.

Appendix A: Acronyms

ARL	Authority Revocation List
CA	Certification Authority
COTR	Contracting Officer’s Technical Representative
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DES	Data Encryption Standard
DN	Distinguished Name
DSA/DSS	Digital Signature Algorithm / Digital Signature Standard
EDI	Electronic Data Interface
FIPS PUB	(US) Federal Information Processing Standard Publication
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
NASA	National Aeronautical and Space Administration
NPG	NASA Procedures and Guidelines
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PA	Policy Authority
RA	Registration Authority
RFC	(IETF) Request For Comments
RSA	Rivest-Shimar-Adleman
SHA-1	Secure Hash Algorithm
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol

Appendix B: Definitions

Activation Data Private data, other than keys, that are required to access cryptographic modules.

Assurance How well a Relying Party can be certain of or trust the certificate.

The level of assurance associated with a public key certificate is an assertion by a CA of the degree of confidence that a Relying Party may reasonably place in the binding of a Subscriber's public key to the identity and privileges asserted in the certificate. Level of assurance depends on multiple factors that include the proper registration of Subscribers, the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of the CP. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates

Authority Revocation List (ARL) A list of revoked CA certificates. An ARL is a CRL for CA cross certificates.

Basic Level of Assurance This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.

CA Signing Key The private portion of the CA signing key pair which is used to digitally sign certificates, certificate revocation lists and authority revocation lists.

CA Signing Key Pair The key pair used by the CA for digitally signing. It consists of the CA signing (private) key and the CA public (I.E. verification) key

CA Public Key The public key portion of the CA signing key pair which is used to verify certificates, certificate revocation lists and authority revocation lists signed by the CA signing key.

Certificate The public key of a user, together with some other information, rendered unforgeable by digitally signing it with the private key of the certification authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509.

Certificate Policy (CP)
A document that defines the policies of a Certificate Authority (CA). A CP addresses all aspects associated with generation, production, distribution, recovery and administration of digital certificates. A CP also defines the policies for administration and operation of a CA.

Certification Practice Statement (CPS)
A statement of practices that a CA employs to implement the specific policies defined in the Certification Policy (CP).

Certificate Revocation List (CRL)
A list of revoked certificates that is created and signed by the same CA that issued the certificates. A certificate is added to the list if it is revoked (e.g., because of suspected key compromise). In some circumstances the CA may choose to split a CRL into a series of smaller CRLs.

Certification Authority
An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.

Cross-certification
The process of establishing a trust relationship between two Certification Authorities. A process by which two Certification Authorities (CAs) securely exchange keying information so that each can certify the trustworthiness of the other's keys. Once the CAs has cross-certified, users within the CA domains can validate each other's certificates.

Digital Signature
The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine:
(a) whether the transformation was created using the key that corresponds to the signer's key; and
(b) whether the message has been altered since the transformation was made.

Directory
A directory system that conforms to the ITU-T X.500 series of Recommendations.

Employee
An employee is any person employed by NASA.

End Entity
An Entity that uses the keys and certificates created within the PKI for purposes other than the management of the aforementioned keys and certificates. An End Entity may be a Subscriber, a Relying Party, a device, or an application.

Entity

Any autonomous element within the Public Key Infrastructure. This may be a CA, a RA or an End Entity.

High Level of Assurance

This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

High-security Zone

An area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors. High-Security Zones should be separated by a perimeter. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.

Issuing CA

In the context of a particular certificate, the issuing CA is the CA that signed and issued the certificate.

Key

In cryptography, a secret value that is used in an encryption algorithm to encrypt and decrypt data.

Key Pair

Two mathematically related keys having the following properties:
1.) one key can be used to encrypt a message that can only be decrypted using the other key
2.) knowing one key, it is computationally infeasible to discover the other key.

MD5

One of the message digest algorithms developed by RSA Data Security Inc.

Medium Level of Assurance

This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

Object Identifier

(OID) The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.

Organization

A department, agency, corporation, partnership, trust, joint venture or other association.

Operational Authority

Personnel who are responsible for the overall operation of a NASA PKI CA. Their responsibility covers areas such as staffing, finances, and dispute resolution. The Operational Authority role does not require an account on the CA workstation.

Policy Authority A NASA body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs throughout the NASA PKI.

Public Key The portion of the public key pair that is available to everyone. The public key is stored in the directory. The NASA PKI uses a public key for encryption and a public (i.e. verification) key for verifying a digital signature.

Public Key Cryptography Public key cryptography is a cryptographic system that uses key pairs. One key of the pair is public and the other key is private and known only to the owner. The mathematical relationship between the keys is such that an action performed by one key (i.e. encryption) can be undone by the other key (i.e. decryption). In addition, the relationship between the keys is such that knowing the public key does not compromise the private key. The NASA PKI uses two key pairs, one pair for encryption and one pair for signing.

Public Key Infrastructure A structure of hardware, software, people, processes and policies that uses Digital Signature technology to provide Relying Parties with a verifiable association between the public component of an asymmetric key pair with a specific Subscriber.

Private Key The portion of the public key pair that is kept secret by the owner of the key pair. The NASA PKI uses a private key for encryption and a private signing key for digital signatures.

Reason Code A code put in the certificate to indicate the reason why the certificate was revoked.

Registration Authority (RA) An Entity that is responsible for the identification and authentication of certificate Subscribers before certificate issuance, but does not actually sign the certificates (i.e., a RA is delegated certain tasks on behalf of a CA).

Relying Party A person who uses a certificate signed by a NASA PKI CA to authenticate a digital signature or to encrypt communications to the certificate subject, and is a Subscriber of a NASA PKI CA or a PKI which is cross certified with the NASA PKI.

Rudimentary Level of Assurance This level provides the lowest degree of assurance concerning identity of the individual. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality.

Sensitive Unclassified

Information, data, or systems that require protection due to the risk and magnitude of the harm or loss that could result from unauthorized disclosure, alteration, loss or destruction but has not been designated as classified for national security purposes.

Sponsor

A Sponsor in the NASA PKI is the NASA department or civil servant that has nominated that a specific individual or organization be issued a certificate. (E.g., for an employee this may be the employee’s manager). The Sponsor is responsible for informing the CA or RA if the relationship with the Subscriber is terminated or has changed such that the certificate should be revoked or updated.

Subscriber

An individual or organization whose public key is certified in a public key certificate. In the NASA PKI this could be a civil servant, or a NASA contractor. Subscribers may have one or more certificates from a specific CA associated with them; most will have at least two active certificates - one containing their Digital Signature key; the other containing their Confidentiality (I.E. encryption) key.

Verification Public Key

The public key portion of a signing key pair used to verify data that has been signed by the corresponding signing private key.

REFERENCES

The documents noted below were referenced in the CPS.

FIPS 112	Password Usage, May 1985.
FIPS 140-1	Security Requirements for Cryptographic Modules, January 1994.
FIPS 186-2	Digital Signature Standard (DSS), January 2000.
NPG 1441	NASA Records Retention and Schedules
NPG 2810.1	Security of Information Technology, August 1999.
PRIVACT	5 U.S.C. 552a, The Privacy Act of 1974.
RFC 2459	X.509 Public Key Infrastructure Certificate and CRL Profile, Housley, Ford, Polk and Solo, January 1999.
RFC 2510	X.509 Public Key Infrastructure Certificate Management Protocols , Adams and Farrell, March 1999.
RFC 2527	X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Chokhani and Ford, March 1999.
X.521	Information Technology-Open Systems Interconnection-The Directory: Selected Object Classes, 1988.
	U.S.C. 2459b, The National Aeronautics and Space Act, as amended.